SEPPMAIL
SWISS E-MAIL SECURITY

SEPPmail

Version 6.5.3

Benutzerhandbuch
mit Ruleset

SEPPmail AG
Industriestrasse 7
CH-5432 Neuenhof

+41 56 648 28 38 fon
+41 56 648 28 39 fax
info@seppmail.ch mail

www.seppmail.ch

Inhaltsverzeichnis

1 Vorwort

Der Inhalt dieses Dokuments kann möglicherweise verändert worden sein, falls Sie es nicht direkt von der SEPPmail AG erhalten haben. Auch wenn dieses Dokument mit der grössten Sorgfalt angefertigt wurde, übernimmt die SEPPmail AG keine Verantwortung für etwaige Fehler oder Unvollständigkeiten. Die Benutzung dieses Dokuments beinhaltet die Zustimmung zu dessen Gebrauch ohne Mangelgewähr und ohne jegliche Garantien. Jeglicher Gebrauch der hier aufgeführten Informationen erfolgt auf eigenes Risiko.

PGP und Pretty Good Privacy sind gesetzlich geschützte Warenzeichen der PGP Corporation, gültig in den USA und anderen Ländern. Java und alle Java-basierten Marken sind Warenzeichen von SUN Microsystems, Inc., gültig in den USA und anderen Ländern. UNIX ist ein eingetragenes Warenzeichen unter der Verfügung der X/Open Company, gültig in den USA und anderen Ländern. Microsoft, Internet Explorer, Windows, Windows NT, Windows 2000 und Windows XP sind entweder eingetragene Warenzeichen oder gesetzlich geschützte Warenzeichen der Microsoft Corporation, gültig in den USA und anderen Ländern. Netscape und Netscape Navigator sind gesetzlich geschützte Warenzeichen der Netscape Communications Corporation, gültig in den USA und anderen Ländern. Alle etwaigen anderen hier aufgeführten Warenzeichen sind Eigentum ihrer jeweiligen Besitzer und werden hier ohne die Absicht der Markenverletzung verwendet.

OpenSSL ist eine Anwendung, die unter einer Apache-ähnlichen Lizenz vertrieben wird (www.openssl.org).
OpenBSD ist ein Betriebssystem, das unter dem Berkeley Copyright vertrieben wird (www.openbsd.org).
GnuPG ist Software, die unter der GNU Public License vertrieben wird (www.gnupg.org).
Der Apache Webserver und Apache Tomcat werden unter dem Apache Software Foundation Copyright entwickelt (www.apache.org).

Hinweise auf kommerzielle Produkte, Verfahren oder Dienstleistungen, durch Nennung des Produkt- oder Herstellernamens oder auf beliebige andere Weise, kommen nicht notwendigerweise einer Billigung, Empfehlung oder Favorisierung durch die SEPPmail AG gleich.

Einfuhr, Ausfuhr und Benutzung dieser und anderer Verschlüsselungsprodukte sind möglicherweise gesetzlich eingeschränkt.

In diesem Dokument vom Verfasser geäusserte Ansichten und Meinungen drücken nicht notwendigerweise jene der SEPPmail AG aus und dürfen nicht zum Zweck der Werbung oder der Produktempfehlung benutzt werden. Verweise auf Internetadressen sind vor der Drucklegung gründlich geprüft worden. Aufgrund des ständigen Wandels der Internetinhalte kann die SEPPmail AG aber keine Garantie für das Vorhandensein und den Inhalt der angegebenen Quellen übernehmen. Sollten Sie in dieser Anleitung fehlerhafte Links finden, teilen Sie uns dies bitte unter Angabe des betroffenen Links und der Versionsnummer dieser Anleitung an die Adresse info@seppmail.ch mit.

Druck: Oktober 2013, CH-5432 Neuenhof

2 Einleitung

Willkommen zur Secure E-Mail Lösung SEPPmail

Das vorliegende Handbuch unterstützt Sie bei Ihrer SEPPmail Installation und dient als Referenz der einzelnen Konfigurationsaspekte. Es ist in folgende drei Teile gegliedert:

Teil I	Der erste Teil besteht aus einer Einführung in das Produkt. Die Funktionsweise und wichtige Produktmerkmale der SEPPmail Appliance werden hier beschrieben.
Teil II	Im zweiten Teil wird erklärt, wie Sie das Secure E-Mail Gateway SEPPmail in Betrieb nehmen. Dies beinhaltet die Integration der Appliance in Ihr Netzwerk sowie die Einrichtung Ihrer Mail- und Netzwerkumgebung.
Teil III	Der dritte und letzte Teil enthält im ersten Abschnitt eine Übersicht der verschiedenen Konfigurationsmöglichkeiten. Die weiteren Kapitel beschreiben Konfigurations- und Administrationsschritte der einzelnen Menüpunkte im Detail. Die Gliederung richtet sich zur einfachen Orientierung nach der Menüstruktur des Web-Administrationsportals.

Wir wünschen Ihnen viel Erfolg bei der Installation.

2.1 Sichere E-Mail-Kommunikation durch Verschlüsselung

SEPPmail setzt auf verschiedene standardisierte Verschlüsselungsverfahren und bietet dadurch höchste Sicherheit für unterschiedliche Kommunikationspartner. In diesem Abschnitt werden die Verfahren erläutert, die dabei zum Einsatz kommen.

Die Secure E-Mail-Gateway Appliance SEPPmail entschlüsselt eingehende E-Mails automatisch. Der Vorgang ist für den E-Mail-Empfänger komplett transparent. Er erhält seine E-Mails unverschlüsselt in seiner Mailbox und liest diese wie bisher, ohne Zusatzaufwand.

Eingehende E-Mails können mit einer digitalen Signatur versehen sein. Bestandteil dieser Signatur ist das öffentliche S/MIME-Zertifikat des Absenders. Um den Verwaltungsaufwand zu minimieren, speichert die SEPPmail Appliance diese S/MIME-Zertifikate automatisch und nutzt sie zur S/MIME E-Mail-Verschlüsselung für entsprechende Kommunikationspartner.

Für den sicheren E-Mail-Versand wählt die SEPPmail-Appliance aus folgenden 5 Methoden die für den Empfänger bestmögliche aus:

1. GINA-Technologie

Bei der GINA-Verschlüsselungstechnologie handelt es sich um ein patentiertes Verfahren. Dabei werden E-Mails nicht bis zur Abholung zwischengespeichert, wie es bei anderen Webmailverfahren üblich ist, sondern vollständig verschlüsselt an den Empfänger ausgeliefert. Dort werden sie in seinem Postfach (z.B. im Outlook) gespeichert. E-Mails sind bei diesem Verfahren vor Phishing-Attacken geschützt, denn neben dem Kennwort ist für den erfolgreichen Zugriff auch die verschlüsselte E-Mail selbst aus der Postfach des Empfängers erforderlich.

Eine GINA-Nachricht enthält die Nachricht in verschlüsselter Form als Dateianlage. Der Empfänger ruft die Nachricht ab, indem er die verschlüsselte Dateianlage im lokalen Webbrowser öffnet. Diese wird dann über eine sichere SSL-Verbindung (HTTPS) an die SEPPmail-Appliance des Absenders übertragen und dort nach Eingabe eines Benutzerkennworts entschlüsselt und angezeigt. Durch die Kennworteingabe wird die Identität des Empfängers bei jedem Abruf geprüft. Im Gegensatz zum herkömmlichen E-Mail-Versand können E-Mail-Zustellungen aufgrund der korrekten Authentifizierung nachgewiesen werden. Die nachfolgende Abbildung zeigt ein Beispiel einer GINA-Nachricht.

Beispiel einer GINA-Nachricht

2. Vollautomatische E-Mail-Domainverschlüsselung zwischen allen SEPPmail Appliances

Die SEPPmail-Appliance bietet Ihnen die Möglichkeit, den E-Mail-Verkehr permanent zwischen mehreren E-Mail-Domains zu verschlüsseln. Einzige Bedingung dabei ist, dass die Kommunikationspartner über je eine SEPPmail-Appliance verfügen. Zwischen den Systemen werden alle Nachrichten automatisch ver- und entschlüsselt. Bei diesem Verfahren kommen sogenannte Domainzertifikate bzw. Domainschlüssel zum Einsatz.

3. S/MIME-Benutzerverschlüsselung

Das Verfahren der Verschlüsselung mittels S/MIME basiert auf öffentlichen und privaten Schlüsseln. M it öffentlichen Schlüsseln werden die E-Mails verschlüsselt und können anschliessend nur mit den zugehörigen privaten Schlüsseln entschlüsselt werden. Dank der zentralen Verarbeitung läuft dieser Vorgang automatisch ab, wenn entsprechende S/MIME Benutzerzertifikate auf der SEPPmail-Appliance existieren. Diese können auf der SEPPmail-Appliance selbst erstellt oder durch einen öffentlichen Zertifikatsanbieter ausgestellt werden. In beiden Fällen lassen sich die Zertifikate automatisiert erstellen. Die SEPPmail-Appliance unterstützt zu diesem Zweck verschiedene Schnittstellen zu öffentlichen Zertifikatsanbietern.

4. OpenPGP-Benutzerverschlüsselung

OpenPGP funktioniert nach dem gleichen Grundprinzip wie S/MIME. Auch die OpenPGP-Schlüssel werden auf der SEPPmail-Appliance verwaltet und E-Mails entsprechend automatisch ver- und entschlüsselt, wenn das benötigte Schlüsselmaterial vorhanden ist. Im Gegensatz zu S/MIME werden die Schlüssel bei OpenPGP immer selbst erzeugt und nicht von unterschiedlichen öffentlichen Zertifizierungsstellen ausgestellt.

5. TLS/SSL Transportverschlüsselung

TLS/SSL bietet eine zusätzliche Sicherheit und ergänzt die bisher beschriebenen Verschlüsselungsmethoden. Die Kommunikation zwischen der SEPPmail-Appliance und anderen E-Mail-Servern wird in der Standardkonfiguration immer über einen TLS/SSL gesicherten Kanal aufgebaut, sofern die Gegenstelle dies unterstützt. Ebenfalls kommt TLS/SSL bei der bereits beschriebenen E-Mail-Domainverschlüsselung zwischen mehreren SEPPmail Appliances zur Anwendung.

2.2 Digitale E-Mail-Signaturen

Beim Einsatz digitaler E-Mail-Signaturen wird die verbindliche E-Mail-Kommunikation gewährleistet, indem die Authentizität einer Nachricht verifiziert werden kann. Es wird somit sichergestellt, dass eine Nachricht unverändert beim Empfänger eintrifft und der angezeigte Absender auch dem tatsächlichen Absender entspricht.

Das Secure E-Mail-Gateway SEPPmail kann Ihre E-Mails entweder mit Benutzer- oder mit Firmen-Zertifikaten signieren. Die beiden Verfahren werden im Folgenden kurz erläutert:

Digitale E-Mail-Signatur mit einem Benutzerzertifikat

Die Signierung der E-Mails mit einem S/MIME-Benutzerzertifikat erlaubt dem Empfänger die Authentizität der E-Mail mit seinem E-Mail-Client zu prüfen. Damit wird sichergestellt, dass der Absender authentisch ist und die E-Mail während und nach dem Versand nicht verändert wurde. Bei dieser Methode wird für jeden E-Mail-Absender ein eigenes S/MIME-Zertifikat benötigt.

Wir empfehlen die Verwendung von Zertifikaten, die durch einen öffentliche Zertifikatsanbieter ausgestellt wurden. Sie können diesen Vorgang automatisieren, indem Sie einen der in die SEPPmail-Appliance integrierten CA-Connectoren zu verschiedenen offiziellen Zertifizierungsstellen verwenden. Die Verbindung der SEPPmail Appliance zu den öffentlichen Zertifikatsanbietern ermöglicht Ihnen eine vollautomatisierte Ausstellung der Zertifikate, ohne Betreuungsaufwand.

Alternativ können E-Mails auch im E-Mail-Client des jeweiligen Absenders signiert werden. Das Secure E-Mail-Gateway SEPPmail wird diese E-Mails dann nur noch verschlüsseln. Viele S/MIME-Zertifikate eignen sich sowohl zum Signieren als auch zum Verschlüsseln. Es kann deshalb sinnvoll sein, die Zertifikate zusätzlich auf der SEPPmail-Appliance zu installieren. Dadurch können E-Mails mit den entsprechenden Zertifikaten automatisch entschlüsselt werden.

Digitale E-Mail-Signatur mit einem Firmenzertifikat

Die Signierung der E-Mails mit einem S/MIME-Firmenzertifikat erfüllt denselben Zweck wie die Signierung mit einem S/MIME-Benutzerzertifikat. Bei dieser Variante wird jedoch nur ein einziges Zertifikat benötigt.

Da S/MIME-Zertifikate grundsätzlich nur für eine E-Mail-Absenderadresse gültig sind, erhalten alle ausgehenden E-Mails den gleichen (technischen) Absender. E-Mails erscheinen beim Empfänger immer mir derselben E-Mail-Adresse, aber korrektem Benutzernamen. Die automatische Erfassung von Kontakten und zugehörigen E-Mail-Adressen funktioniert dadurch beim Empfänger nicht mehr wie erwartet. Ebenso sind an anderen Stellen Schwierigkeiten zu erwarten. So besteht z.B. die Gefahr, dass alle Ihre Firmen-E-Mails abgewiesen werden, wenn die verwendete Absenderadresse beim Empfänger fälschlich als SPAM eingestuft wird.

2.3 Zentraler Firmen E-Mail-Disclaimer

Das Secure E-Mail-Gateway SEPPmail kann Ihre E-Mails mit einem Firmen E-Mail-Disclaimer ergänzen. Es werden Disclaimer im Text- oder HTML-Format unterstützt.

Nutzen Sie den zentralen Firmendisclaimer, um einen einheitlichen Text oder Angaben wie Adresse und Firmeninhaber an alle E-Mails anzuhängen.

Beispiel im Textformat:

```
Firma AG - Musterstrasse 1, 1234 Musterstadt - www.meinefirma.ch
```

2.4 E-Mail-Contentprüfung durch Virus, Spam and Phishing Protection (Protection Pack)

SEPPmail-Protection Pack (Virus, SPAM and Phishing Protection) ist als Option erhältlich und schützt Sie vor SPAM (unerwünschten E-Mails), Viren (schädlichen E-Mails) und Phishing-E-Mails (gefälschten E-Mails).

Die Antivirus-Komponente aktualisiert konfinuierlich ihre Virendefinitionen und führt automatisch Virenprüfungen Ihrer E-Mails durch.

SPAM-E-Mails werden durch den integrierten und einfach zu konfigurierenden SPAM-Filter wirksam bekämpft. Dieser basiert auf der Kombination verschiedener Filtertechniken wie Greylisting, Blacklisting, Bayes'sche Filter und SMTP-Protocol-Checks.

Phishing-Attacken werden durch GINA-Nachrichten verhindert, indem der Empfänger sowohl die verschlüsselte Nachricht selbst wie auch ein Kennwort zum Abruf benötigt.

Hinweis beim Einsatz mit bestehenden Antiviren-Systemen

Die SEPPmail-Appliance kann auch mit bereits vorhandenen Antiviren-Systemen eingesetzt werden. Beachten Sie jedoch, dass SEPPmail die E-Mails verschlüsselt versendet/empfängt.

Um E-Mails auf Viren zu überprüfen müssen diese in unverschlüsselter Form vorliegen. Führen Sie deshalb die Virenprüfung nach der Entschlüsselung in Ihrem internen Netzwerk durch (z.B. auf Ihrem internen E-Mail-Server), falls Sie Ihr bestehendes Antiviren-Produkt weiterhin einsetzen möchten.

2.5 Kompatibilität zu anderen Secure E-Mail Systemen

Aufgrund der zentralen E-Mail-Verarbeitung und Schlüsselverwaltung lässt sich SEPPmail transparent in Ihre E-Mail-Infrastruktur integrieren. Alle anerkannten und sicheren Standard-Verschlüsselungstechniken sind implementiert. Die Kompatibilität zu den gängigen Secure E-Mail-Systemen ist damit sichergestellt und die Installation zusätzlicher Softwarekomponenten entfällt.

Für Empfänger, die keine S/MIME-Zertifikate oder OpenPGP-Schlüssel besitzen, kann die GINA-Technologie zur sicheren E-Mail-Übertragung genutzt werden.

2.6 Remote-Administration mittels Web-Portal

Sämtliche Verwaltungsmöglichkeiten des SEPPmail Secure E-Mail-Gateways stehen über eine webbrowserbasierten Konfigurationsoberfläche zur Verfügung. Die Verbindung zwischen Webbrowser und dem SEPPmail Secure E-Mail-Gateway ist zusätzlich verschlüsselt (HTTPS).

3 Inbetriebnahme der Secure E-Mail-Gateway-Appliance

3.1 Bevor Sie beginnen

Bitte überprüfen Sie den Verpackungsinhalt auf Vollständigkeit. Der Lieferumfang besteht aus:

Anzahl	Beschreibung
1	SEPPmail-Hardware-Appliance bzw. SEPPmail-Virtual-Appliance für VMware ESX oder Microsoft Hyper-V Server
1	Quick Install Guide
1	Kaltgerätekabel (240V)

Sollte der Lieferumfang bei Ihnen unvollständig sein oder sollten bei der Installation der SEPPmail-Appliance Probleme oder Fragen auftauchen, kontaktieren Sie bitte SEPPmail oder Ihren SEPPmail Fachhändler.

Eine Liste mit den Kontaktangaben der jeweiligen Fachhändler finden Sie auf der Webseite der SEPPmail AG - http://www.seppmail.ch.

3.2 Integration der Appliance in Ihre E-Mail-Umgebung (Standard Konfiguration)

In diesem Abschnitt wird ein einfaches Szenario beschrieben, in dem die SEPPmail-Appliance externe E-Mails aus dem Internet direkt entgegennimmt und interne E-Mails nach extern ins Internet versendet. Je nach Aufbau Ihrer E-Mail-Infrastruktur können weitere E-Mail-Server oder Gateways im E-Mail-Datenfluss vorkommen.

In diesem Szenario wird SEPPmail als SMTP-Gateway zwischen dem Internet und Ihrem internen E-Mail-Server installiert. Dadurch ändert sich der E-Mail-Datenfluss in den folgenden zwei wesentlichen Punkten:

1. E-Mails aus dem Internet werden nicht mehr direkt an internen Ihren E-Mail-Server, sondern (neu) an die SEPPmail-Appliance gesendet.

2. Ihr E-Mail-Server schickt seine E-Mails nicht mehr direkt ins Internet, sondern (neu) an die SEPPmail -Appliance. Die SEPPmail-Appliance übernimmt somit eine Smarthost-Funktion.

Die E-Mail-Infrastruktur für den beschriebenen Aufbau sehen Sie in nachfolgender Abbildung.

Typischer Aufbau einer E-Mail-Infrastruktur mit einer SEPPmail Appliance

3.3 Benötigte Informationen zur Inbetriebnahme

Es wird empfohlen, folgende Informationen Ihrer E-Mail-Umgebung zusammenzustellen, bevor Sie mit der Inbetriebnahme beginnen:

Benötigte Information	Ihre Angabe
Öffentlicher DNS-Eintrag oder öffentliche IP-Adresse der Appliance*: Dies ist der Name oder die IP-Adresse, unter der Ihre SEPPmail-Appliance aus dem Internet erreichbar sein wird.	
Interne IP-Adresse der Appliance: Die interne IP-Adresse und Subnetzmaske, unter der die SEPPmail-Appliance in Ihrem internen Netzwerk erreichbar sein wird.	
Hostname der Appliance: Ein frei wählbarer Hostname Ihrer SEPPmail-Appliance, z.B. secureemailgateway. Dieser ist normalerweise im DNS Server aufgeführt.	
Interne Domain, in welcher sich die SEPPmail-Appliance befindet: Beispiele sind: ihrefirma.local oder ihredomain.de usw.	
Standard Gateway IP-Adresse: Dies ist die Standard-Gateway IP-Adresse Ihrer Firewall oder Ihres Routers, über welche die SEPPmail-Appliance die Verbindung mit dem Internet herstellen kann.	
DNS Server: Hier können Sie bis zu drei IP-Adressen von DNS-Servern eingeben. Es kann sich sowohl um interne wie auch um externe DNS-Server handeln. Interne DNS-Server müssen Anfragen für externe Adressen entsprechend weiterleiten.	
Hostname oder IP-Adresse des bestehenden internen E-Mail-Servers: Hostname oder IP-Adresse, unter der Ihr bestehender interner E-Mail-Server im internen Netzwerk angesprochen werden kann.	
E-Mail-Domains: Geben Sie hier die Domains der E-Mail-Adressen Ihrer Organisation an, z.B. firma.ch, firma.com, firma.de.	

Benötigte Informationen zum Einrichten der SEPPmail Appliance

* Die SEPPmail-Appliance muß aus Internet als Webserver erreichbar sein und benötigt deshalb eine von extern erreichbare IP-Adresse. Oft ist dies die Adresse der Firewall oder einer Reverse-Proxies /

Web-Application-Firewall. In einfachen Installationen kann dazu die IP-Adresse verwendet werden, unter der Ihr Internet-Router von extern erreichbar ist.

Sie finden diese Information mit folgenden Schritten:

1. Öffnen Sie auf einem Windows-PC eine Eingabeaufforderung und geben Sie den Befehl "`nslookup`" ein und drücken Sie Enter.
2. Geben Sie nach dem ">" Zeichen (Prompt) "`set querytype=mx`" ein und bestätigen Sie mit Enter.
3. Geben Sie die E-Mail-Domain Ihrer Organisation ein (z.B. ihredomain.com) und bestätigen Sie mit Enter.
4. Sie erhalten eine oder mehrere Antworten mit dem Begriff "`mail exchanger =`"

Servernamen hinter dem Begriff "`mail exchanger`" mit der geringsten MX-Preference-Nummer haben die höchste Priorität bei der Namensauflösung.

3.4 SEPPmail-Appliance anschliessen

Falls Sie die VM-Version (Virtual Machine) der SEPPmail-Appliance erworben haben, starten Sie Ihre virtuelle-Appliance.

Wenn Sie die Hardware-Version besitzen, schließen Sie die SEPPmail-Appliance wie folgt an:

1. Verbinden Sie die mit »LAN1« oder »eth0« gekennzeichnete Ethernet-Schnittstelle der SEPPmail-Appliance mit der Ethernet-Schnittstelle Ihres Computers. Benutzen Sie dazu ein gekreuztes RJ45 Patchkabel (auch bekannt als Crossover-Kabel). Alternativ können Sie einen Ethernet-Hub oder Ethernet-Switch mit einem normalen RJ45 Patchkabel verwenden.

2. Schließen Sie die Appliance mittels beiliegendem Stromkabel an das Stromnetz an.

3.5 Firewall / Router einrichten

Definieren Sie auf Ihrer Firewall bzw. Ihrem Internet-Router folgende Regeln, um die sichere E-Mail-Kommunikation durch SEPPmail zu gewährleisten:

Port	Quelle	Ziel	Beschreibung	
TCP/22 (SSH)	Appliance	Internet	Ermöglicht es, Updates der Appliance durchzuführen und kommt bei Support Sitzungen zum Einsatz.	
TCP/22 (SSH)	Appliance	Appliance	Wird beim Betrieb mit mehreren Appliances im Clusterverbund benötigt.	**
TCP/25 (SMTP)	E-Mail-Server	Appliance	Wird benötigt, damit der interne E-Mail-Server ausgehende E-Mails an die Appliance senden kann, die dort verschlüsselt oder signiert werden.	
TCP/25 (SMTP)	Internet	Appliance	Ermöglicht den E-Mail-Verkehr zwischen Internet und Appliance.	
TCP/25 (SMTP)	Appliance	Internet	Wird für das direkte Versenden von E-Mails ins Internet benötigt.	
		E-Mail-Server	Wird für das Versenden von E-Mails an einen internen E-Mail Server benötigt.	**
UDP/53 (DNS) TCP/53 (DNS)	Appliance	Nameserver (intern)	Ermöglicht die Namensauflösung, wenn interne DNS-	**

Port	Quelle	Ziel	Beschreibung	
			Server verwendet werden.	
		Nameserver (extern)	Ermöglicht die Namensauflösung, wenn externe DNS-Server verwendet werden.	
		Internet	Ermöglicht die Namensauflösung, wenn die Einstellung »built-in DNS Resolver« verwendet wird.	
TCP/80*	Appliance	Internet	Wird für Protection Pack (Virus, SPAM and Phishing Protection) Updates benötigt.	
TCP/443 (HTTPS)	Internet	Appliance	Stellt die verschlüsselte Kommunikation über SSL (HTTPS) zu SEPPmail her. Wird für die Nutzung der GINA-Technologie benötigt.	
UDP/6277*	Appliance	Internet	Wird für Protection Pack mit DCC benötigt.	
UDP/24441*	Appliance	Internet	Wird für Protection Pack mit Pyzor benötigt.	
TCP/UDP/123* (NTP)	Appliance	Internet	Ermöglicht die Zeitsynchronisation.	
TCP/8080* (HTTP) und/ oder TCP/8443* (HTTPS)	Admin PC	Appliance	Stellt den Administratoren-Zugang im internen Netz sicher. Es wird empfohlen, nur die SSL-verschlüsselte Verbindung (HTTPS) über Port TCP/8443 zuzulassen.	**
TCP/5061*	Appliance	Internet	Wird für den SMS-Versand via verwendet.	

Regeln zur Gewährleistung der Netzwerkkommunikation der SEPPmail Appliance

* optional, je nach Konfiguration der SEPPmail-Appliance
** In einfachen Installationen wird keine Firewall zwischen der SEPPmail-Appliance und dem internen Netz verwendet. Die mit ** markierten Regeln entfallen dann.

3.6 Netzwerkeinstellungen und Systemregistrierung

Nachfolgend wird beschrieben, wie Sie Ihre SEPPmail Appliance in Ihr Netzwerk integrieren und die Netzwerkkommunikation prüfen können. Dazu gehören die Definition der IP-Adresse(n) Ihrer SEPPmail-Appliance, DNS-Einstellungen, Eingabe des Standard-Gateways, die Vergabe eines Hostnamen und die Angabe Ihrer internen Domain.

Zum Abschluß können Sie prüfen, ob die Einstellungen korrekt sind, indem Sie die Funktion »Check Update« der Appliance nutzen und Ihr System registrieren.

3.6.1 Installations-PC einrichten

Zur erstmaligen Konfiguration der Netzwerkparameter Ihrer SEPPmail-Appliance muss sich Ihr Computer im selben Netzwerk wie die Appliance selbst befinden. Falls sich dieser nicht bereits im IP-Adressenbereich 192.168.1.xxx/24 befindet, ändern Sie die IP-Adresse Ihres Computers auf eine IP-Adresse zwischen 192.168.1.1/24 - 192.168.1.254/24, Netwerkmaske 255.255.255.0.

Hinweis:

Verwenden Sie nicht die Adresse 192.168.1.60, diese ist für die SEPPmail-Appliance reserviert. Dies ist die Standard IP-Adresse im Auslieferungszustand.

Ein Beispiel entsprechender Netzwerkeinstellungen sehen Sie in nachfolgender Abbildung.

Eigenschaften von Internetprotokoll Version 4 (TCP/IPv4)

Allgemein

IP-Einstellungen können automatisch zugewiesen werden, wenn das Netzwerk diese Funktion unterstützt. Wenden Sie sich andernfalls an den Netzwerkadministrator, um die geeigneten IP-Einstellungen zu beziehen.

IP-Adresse automatisch beziehen

Folgende IP-Adresse verwenden:

IP-Adresse: 192 . 168 . 1 . 10

Subnetzmaske: 255 . 255 . 255 . 0

Standardgateway: . . .

DNS-Serveradresse automatisch beziehen

Folgende DNS-Serveradressen verwenden:

Bevorzugter DNS-Server: . . .

Alternativer DNS-Server: . . .

Einstellungen beim Beenden überprüfen

Erweitert...

OK Abbrechen

3.6.2 Login als Administrator

Sämtliche Verwaltungsmöglichkeiten der SEPPmail-Appliance stehen über eine webbrowserbasierten Konfigurationsoberfläche zur Verfügung. Im Auslieferungszustand können Sie die Konfigurationsoberfläche unter der folgenden Adresse erreichen:

LAN1 - https://192.168.1.60:8443
LAN2 - https://192.168.2.60:8443

Der Standard-Benutzername lautet : admin
Das Standard-Kennwort lautet : admin

Hinweis:

Sie erhalten in diesem Stadium die Meldung »No valid license found - Please obtain a valid license«, da die SEPPmail-Appliance mit einer temporären Lizenz ausgeliefert wird. Folgen Sie den weiteren Anweisungen in diesem Kapitel, um Ihr System grundlegend einzurichten und zu registrieren. Dadurch erhalten Sie eine permanente Lizenz und können die SEPPmail-Appliance in vollem Umfang nutzen.

Beim Aufruf der Konfigurationsoberfläche im Webbrowser erhalten Sie eine Fehlermeldung mit dem Hinweis, daß das SSL-Zertifikat der Webseite ungültig ist. Wählen Sie die Option, diese Seite trotzdem aufzurufen.

Hinweis:

Die Meldung erscheint nur anfänglich, bis ein gültiges SSL-Zertifikat installiert wurde (siehe Menüpunkt »SSL« 106).

3.6.3 Netzwerkeinstellungen der SEPPmail-Appliance

Um die Netzwerkparameter Ihrer SEPPmail Appliance zu konfigurieren, klicken Sie in der Konfigurationsoberfläche auf den Menüpunkt »System«.

Sektion »IP Addresses«

Parameter	Beschreibung
Interface 1 - IP-Adresse	IP-Adresse im Netzwerk für die Schnittstelle »LAN1« bzw. »eth0«
Netzmaske	Netzwerkmaske zur IP-Adresse der Schnittstelle

Hnweis:

Die Definition der Netzmaske wird nach der Classless Inter-Domain Routing (CIDR) Notation festgelegt.
- Die Netzmaske 255.255.255.255 entspricht "/32" (einzelne IP-Adresse)
- Die Netzmaske 255.255.255.0 entspricht "/24" (Klasse-C Netzwerk)
- Die Netzmaske 255.255.0.0 entspricht "/16" (Klasse-B Netzwerk)
- Die Netzmaske 255.0.0.0 entspricht "/8" (Klasse-A Netzwerk)

Sektion »DNS«

Parameter	Beschreibung
Primary	IP-Adresse des DNS-Servers Hinweis: Bitte stellen Sie sicher, dass die DNS-Einträge korrekt sind. Domainnamen im Internet sollten durch die eingetragenen DNS-Server aufgelöst werden können. Falsche Einträge können zu einem sehr langsamen Antwortverhalten der Konfigurationsoberfläche führen, so dass das Laden von Menüpunkten mehrere Minuten dauern kann. Sie können alternativ die Einstellung »Use built-in DNS Resolver« verwenden. Falls Sie diese Option verwenden, stellen Sie sicher, dass Sie Ihre Firewall bzw. Ihren Router so einrichten, dass die SEPPmail-Appliance DNS-Auflösungen via Root-DNS-Server im Internet ausführen kann (vgl. Abschnitt Firewall / Router einrichten 18).
Alternate 1	IP-Adresse eines weiteren DNS-Servers, falls der primäre DNS-Server nicht antwortet

3.6.4 Host- und Domainnamen vergeben

Um den Host- und den Domainnamen Ihrer SEPPmail Appliance zu konfigurieren, klicken Sie in der Konfigurationsoberfläche auf den Menüpunkt »System«. Geben Sie die entsprechenden Werte in den Feldern »Hostname« und »Domain« ein.

Den Hostnamen können Sie frei wählen, z.B. securemailgateway. Der Domainname entspricht der DNS-Domain, in welcher sich die Appliance befindet (z.B. ihrefirma.local oder ihredomain.com). Diese Einstellungen sind die interne Sicht, sie müssen also nicht den Daten, wie sie vom Internet her Gültigkeit hätten, entsprechen.

3.6.5 Netzwerkkonfiguration prüfen

Führen Sie folgende Schritte durch, um sicherzustellen, dass die SEPPmail-Appliance mit den von Ihnen vorgenommenen Netzwerkeinstellungen funktioniert:

1. Klicken Sie in der Konfigurationsoberfläche auf den Menüpunkt »Administration«.
2. Klicken Sie auf die Schaltfläche »Check for Update«.

Falls Sie eine der beiden folgenden Meldungen erhalten, war die Netzwerkkonfiguration erfolgreich:

- »You already have the latest version installed«
- »There is a new version available: Installed version is alteVersionsnummer, latest

version is neueVersionsnummer«

Andernfalls erscheint die Meldung »ERROR: unable to connect to update server. make sure that the device can make connections to the internet on port 22«. Sollte diese Meldung erscheinen, prüfen Sie nochmals, ob Ihre Netzwerkeinstellungen korrekt sind und, ob Ihre Firewall bzw. Ihr Router die Verbindung von Ihrer Appliance ins Internet über Port TCP/22 (SSH) zulässt (vgl. Abschnitt Firewall / Router einrichten18).

3.6.6 Das System auf den neusten Stand bringen

Klicken Sie im Web-Administrationsportal auf den Menüpunkt »Administration« und dann auf die Schaltfläche »Check for Update«. Falls ein Update zur Verfügung steht, klicken Sie zusätzlich auf die Schaltfläche »Fetch Update«. Dies kann zeitaufwändig sein, wenn das gelieferte System noch eine ältere Firmware enthält und deshalb mehrere Updates durchführen muß.

Wiederholen Sie den Schritt, bis keine Updates mehr angezeigt werden. Das System optimiert diesen Prozess, so dass nicht für jede Zwischenversion ein Update durchgeführt werden muss, sondern nur für diejenigen, welche die Datenstruktur verändern.

Es kann unter Umständen vorkommen, dass Sie längere Zeit keine Rückmeldung erhalten. Wenn dies der Fall ist, aktualisieren Sie die Ansicht, indem Sie auf den Link »System Administration« oberhalb der Schaltflächen klicken. Solange Sie nicht ausgeloggt wurden, ist das Update noch nicht abgeschlossen.

Die SEPPmail-Appliance muss nach Updates jeweils einen Neustart durchführen. Sie müssen sich neu anmelden. Führen Sie diesen Schritt gegebenenfalls selbst durch, falls das System lange keine Rückmeldung gibt, Ihnen also nicht die Loginmaske angezeigt wird. Sie können den Neustart auslösen, indem Sie innerhalb des Menüs »Administration« auf die Schaltfläche »Reboot« klicken und danach den angezeigten Sicherheitscode bestätigen. Prüfen Sie nach dem Neustart jeweils erneut, ob weitere Updates zur Verfügung stehen.

Wenn Sie die Meldung »You already have the latest version installed« sehen, ist Ihre SEPPmail -Appliance auf dem neusten Stand. Sollten in Zukunft weitere Updates verfügbar sein, wird dies nach einem Neustart jeweils automatisch angezeigt.

3.6.7 Das System registrieren

Registrieren Sie Ihr System, damit Sie eine permanente Lizenz erhalten. Klicken Sie im Web-Administrationsportal auf den Menüpunkt »Administration« und dann auf die Schaltfläche »Register this device...«.

Es erscheint ein Registrierungsfenster. Füllen Sie die Felder im Registrierungsfenster mit Ihren Angaben aus. Geben Sie in der oberen Hälfte Ihre Kundeninformationen und in der unteren Hälfte die Daten Ihrer Bezugsquelle ein. Schließen Sie die Eingaben ab, indem Sie auf die Schaltfläche »Send« klicken.

Erscheint die Meldung »Registration successful«, haben Sie den Registrierungsvorgang erfolgreich abgeschlossen.

3.7 Wichtige Sicherheitsmassnahmen

In den kommenden Abschnitten werden folgende Sicherheitsmaßnahmen beschrieben:

Ändern des Administrator-Passworts 24
Festlegen des HTTPS-Protokolls für den sicheren Zugriff auf die Appliance 24
Erstellen eines Backup Users zur regelmässigen Sicherung der Appliance 24

3.7.1 Administrator-Kennwort ändern

Bitte stellen Sie sicher, dass das Kennwort des Benutzers »admin« geändert und auf einen entsprechend komplexen Wert gesetzt wird. Melden Sie sich als Benutzer »admin« am System an und klicken Sie auf das Menü »Users«. Wählen Sie dort den Benutzer »admin« aus. Dort können Sie das Kennwort ändern und bei Bedarf weitere Einstellungen vornehmen, die den Benutzer »admin« betreffen.

3.7.2 Festlegen des HTTPS-Protokolls für den sicheren Zugriff zum System

Unter dem Menüpunkt »System« finden Sie die Schaltfläche »Advanced View« Klicken Sie auf diese, um weitere Konfigurationsoptionen aufzurufen. In den Sektionen »GUI Protocol« und »GINA https Protocol« können Sie einstellen, ob entsprechende Zugriffe auf die Appliance mittels HTTP oder HTTPS erfolgen sollen.

Aus Sicherheitsgründen wird empfohlen, die Option HTTP zu deaktivieren und sowohl für die Konfigurationsoberfläche »GUI Protocol« wie auch für »GINA https Protocol« nur HTTPS zuzulassen.

3.7.3 Backup Benutzer erstellen

Um die Konfiguration der SEPPmail-Appliance regelmässig zu sichern, legen Sie hierfür einen Backup Benutzer an. Das Backup der Appliance wird täglich verschlüsselt und an die E-Mail-Adressen aller Backup Benutzer gesendet.

Klicken Sie zur Erstellung eines Backup Benutzers auf den Menüpunkt »Users« und dann auf die Schaltfläche »Create new user account...«. Füllen Sie die Felder »User ID«, »Full Name«, »E-Mail« und »Password« aus. Stellen Sie sicher, dass es sich bei der E-Mail-Adresse um eine gültige Adresse handelt. Klicken Sie das Menü »Groups«. Im Bereich »backup (Backup Operator)« klicken Sie auf die Schaltfläche »Edit...«. Fügen Sie die benötigten Benutzer der Liste der Gruppenmitglieder hinzu.

Backup Kennwort setzen

Damit die Datensicherung der Appliance durchgeführt werden können, muss zusätzlich ein Backup-Kennwort gesetzt werden. Backups der Appliance werden mit diesem Kennwort verschlüsselt. Bei einer Wiederherstellung der Appliance durch Import einer Backupdatei muss dieses Kennwort eingegeben werden.

Um das Kennwort zu setzen, klicken Sie auf den Menüpunkt »Administration« und anschließend auf die Schaltfläche »Change Password« in der Sektion »Backup«.

3.8 Weitere Schritte

Sie haben nun die Grundlage für den sicheren E-Mail-Verkehr durch die SEPPmail-Appliance geschaffen.

Führen Sie folgenden 5 Schritte durch, um eine Minimalkonfiguration zum sicheren E-Mail-Austausch zu erreichen:

1. Datum und Zeit einstellen und NTP-Synchronisation einrichten 52
2. Zu verwaltende E-Mail-Domains einrichten 60
3. E-Mail-Relay Einstellungen 63
4. SSL-Zertifikat selbst erstellen 106 (für den Testbetrieb)
5. SSL-Zertifikat von einer öffentlichen Zertifizierungsstelle anfordern 108 (für den Produktivbetrieb)

Die folgenden beiden Punkte werden im Anschluß beschrieben.

Führen Sie diese jedoch erst nach den vorangehenden Schritten durch, um den E-Mail-Verkehr nicht zu beeinträchtigen.

1. E-Mail-Datenfluss umstellen 25
2. E-Mail-Clients verwenden 27

3.8.1 E-Mail-Datenfluss umstellen

Um den sicheren E-Mail-Verkehr mit der SEPPmail-Appliance zu ermöglichen, müssen Sie folgende Änderungen an Ihrem bestehenden E-Mail-Server vornehmen:

1. Autorisierung der SEPPmail-Appliance für den E-Mail-Versand mittels E-Mail-Relay-Einstellung
2. SEPPmail-Appliance als Smarthost definieren

Stellen Sie sicher, dass der E-Mail-Verkehr mittels SEPPmail-Appliance nach extern möglich ist, indem Sie Ihre Firewall bzw. Ihren Router wie zuvor beschrieben einrichten (siehe Abschnitt Firewall / Router einrichten 18).

Sobald Sie die SEPPmail-Appliance in Ihren E-Mail-Datenfluss integrieren, müssen Sie zudem die IP-Adresse Ihres bestehenden E-Mail-Servers in Ihren Firewall-Regeln durch die IP-Adresse der Appliance ersetzen.

Sobald Sie die SEPPmail-Appliance in Ihren E-Mail-Datenfluss integrieren, müssen Sie dafür sorgen, dass die E-Mails von extern nicht mehr zum E-Mail-Server, sondern zu SEPPmail transportiert werden. Dies kann in der Firewall oder einem vorgelagerten SPAM-Filter eingerichtet werden, je nach Ihrer Netzwerkinfrastruktur.

In der Standardeinstellung versendet SEPPmail E-Mails direkt ins Internet. Falls der E-Mail-Verkehr über einen SMTP-Gateway (Relay) erfolgen soll, richten Sie Ihre Appliance entsprechend ein (siehe Ausgehenden Mailverkehr steuern 60).

Autorisierung für den E-Mail-Versand

Um die E-Mail-Übermittlung von Ihrer SEPPmail-Appliance an Ihren bestehenden E-Mail-Server zu ermöglichen, müssen Sie die Appliance dafür autorisieren. Diese Einstellung ist meist als SMTP E-Mail-Relaying definiert. Tragen Sie hierfür die interne IP-Adresse oder den internen Hostnamen der SEPPmail-Appliance auf Ihrem E-Mail-Server in die Liste der autorisierten E-Mail-Relay Systeme ein.

Definition der SEPPmail-Appliance als Smarthost

Die SEPPmail Appliance wird nach der Integration in Ihre E-Mail-Umgebung die Rolle eines SMTP-Gateways übernehmen. Ihr E-Mail-Server übermittelt E-Mails dann nicht mehr direkt nach extern, sondern (neu) an die SEPPmail-Appliance.

Um diese Änderung vorzunehmen, definieren Sie den internen Hostnamen bzw. die interne IP-Adresse Ihrer SEPPmail-Appliance auf Ihrem bestehenden E-Mail-Server als Smarthost.

ACHTUNG

Mit dieser Anpassung ändern Sie die E-Mail-Kommunikation, indem Sie die SEPPmail-Appliance in den E-Mail-Datenfluss integrieren. Alle E-Mails werden nach der Umstellung an die SEPPmail-Appliance gesendet.

Führen Sie diese Umstellung erst dann durch, wenn alle anderen Konfigurationsschritte der SEPPmail-Appliance abgeschlossen sind. Es kann sonst zu einer Beeinträchtigung des E-Mail-Verkehrs kommen.

3.8.2 E-Mail-Clients verwenden

Der Einsatz standardisierter Verfahren und die zentrale Verarbeitung durch die SEPPmail-Appliance stellt die Unabhängigkeit vom lokalen E-Mail-Client sicher. Es sind deshalb keinerlei Anpassungen der E-Mail-Clients erforderlich.

Der Benutzer hat innhalb seines E-Mail-Clients die folgenden Steuerungsmöglichkeiten, um E-Mails verschlüsselt zu versenden:

- Wählen Sie in MS-Outlook die Nachrichtenoption »Vertraulich«.
- Geben Sie alternativ in der Betreffzeile das Tag [secure] ein. Dies ist der im Standard definierte Begriff, welcher einen verschlüsselten E-Mail-Versand auslöst.

Neben dem Tag [secure] stehen weitere Begriffe zur Verfügung, beispielsweise zur Signierung von E-Mails. Sie können die Begriffe in der Konfigurationsoberfläche im Menü »Mail Processing« in der Sektion »Ruleset Generator« einsehen und bei Bedarf anpassen. Für weitere Details, siehe Abschnitt Regelwerk verwalten 92.

Nachrichtenoption »Vertraulich« in Outlook

4 Microsoft Outlook Add-In

4.1 Einleitung

Das SEPPmail-Add-In für Microsoft Outlook kann auf PC-Systemen mit Microsoft Outlook installiert werden. Die Installation kann mit Benutzerdialog oder im Silent-Mode ohne Benutzerdialog erfolgen. Je nach gewählter Installation stehen unterschiedliche Einstellungen (Parameter) zur Verfügung, um die Funktionalität des Add-Ins zu beeinflussen.

Das Add-In selbst stellt in jeder Art von E-Mail-Fenster (zum Verfassen einer E-Mail) definierbare Schaltflächen zur Verfügung. Abhängig von den bei der Installation gewählten Einstellungen sind es unterschiedlich viele Schaltflächen, mit unterschiedlichen Standard-Einstellungen (gedrückt / nicht gedrückt).

Die Zustände der Haupt-Schaltflächen beim späteren Versenden einer E-Mail werden in Form von Steuer-Informationen in den Header der E-Mail integriert und vom zentralen SEPPmail-System ausgewertet. Eine (optionale) Schaltfläche ruft eine Hilfe-Seite im Standard-Webbrowser auf. Durch eine (optionale) Einstellung kann eine Warnung beim Versenden von unverschlüsselten und unsignierten E-Mails erscheinen.

Die Anwendung ist mehrsprachig und paßt sich der jeweiligen Sprache der Microsoft Outlook-Oberfläche an. Ist diese nicht verfügbar, wird Englisch als Standardsprache für das Add-in verwendet.

Im Folgenden werden technische Details zu den System-Anforderungen, zur Installation, zu den Abläufen in der Registry und zum Versand von E-Mails beschrieben.

4.2 Systemanforderungen

Das SEPPmail-Add-In für Microsoft Outlook kann unter verschiedenen Betriebssystemen und Microsoft Outlook Versionen installiert werden:

Microsoft Windows Betriebssysteme:

- Windows XP
- Windows Vista
- Windows 7 (32bit und 64bit)
- Windows Terminal Server

Microsoft Outlook Versionen:

- Outlook 2000
- Outlook XP
- Outlook 2003
- Outlook 2007
- Outlook 2010(32bit)
- Outlook 2010(64bit)

.NET Framework:

Das .NET Framework muss in der Version 3.5 SP1 oder neuer vorhanden sein. Fehlt dieses, versucht die Installationsroutine diese Komponente automatisch aus dem Internet zu beziehen und zu installieren.

4.3 Download

Das SEPPmail-Add-In für Microsoft Outlook können Sie auf der folgenden Webseite in der jeweils aktuellen Version herunterladen:

http://dl.seppmail.ch

4.4 Installation

Die Installation besteht aus zwei Dateien:

`Setup.exe`

- Ist erforderlich um auf Windows Vista und Windows 7, bei eingeschaltetem UAC, per Rechtsklick »`Als Administrator`« auswählen zu können.
- Prüft vor dem Ausführen der .msi-Datei, ob die Voraussetzungen für die Installation (z.B. NET Framework) vorhanden sind.

`SecureMailAddInSetup 1.2.6.msi`

- Führt die eigentliche Installation durch.
- Kann auch direkt gestartet werden, wenn entsprechende Rechte vorhanden sind (z.B. inaktives UAC und Administrator-Rechte).
- Kann auch für die automatisierte Software-Verteilung verwendet werden.

4.4.1 Installation mit Benutzeroberfläche

Beispiel: Windows 7 (64bit)

1. Rechtsklick auf die Datei »setup.exe« und auswählen der Option »Als Administrator ausführen«.

Installation - Outlook Add-In

2. Die Sicherheitsabfrage von Windows mit »Ja« beantworten, um die Installation zu starten.
3. Im Folgenden erscheinen die folgenden Bildschirme auf denen der Benutzer Wahlmöglichkeiten hat:
   a. zu den später angezeigten Schaltflächen
   b. zum Ein- und Ausschalten einer Warnung beim Versand von unverschlüsselten und unsignierten E-Mails
   c. zu den Standard Schaltflächen-Zuständen bei Öffnen eines E-Mail-Fensters

Installation - Outlook Add-In - angezeigte Schaltflächen - Warnmeldung

SEPPmail Outlook Add-In

SEPPMAIL
SWISS E-MAIL SECURITY

Start Outlook with buttons activated:

- [ ] Button: Encrypt
- [ ] Button: Add signature
- [ ] Button: Encrypt with read receipt

Cancel | < Back | Next >

Installation - Outlook Add-In - aktive Schaltflächen

SEPPmail Outlook Add-In

Installation Complete

SEPPmail Outlook Add-In has been successfully installed.

Click "Close" to exit.

The installatiion was successful.

Cancel | < Back | Close

Installation erfolgreich abgeschlossen - Outlook Add-In

4.4.2 Installation ohne Benutzeroberfläche

Alternativ kann die Installation über die Eingabeaufforderung mit diversen Parametern gestartet werden.

Hinweis:

Die Eingabeaufforderung muss als Administrator gestartet werden!

Beispiel: (Aufruf als einzelne Befehlszeile)

```
msiexec /q /i "SecureMailAddInSetup 1.2.6.msi" SMWarning=false
SMEncrypt=true SMSign=true SMWebmail=true SMHelp=true
SMEncryptSelected=false SMSignSelected=false SMWebmailSelected=false
/li .\log.txt
```

Msiexec-Parameter:

Parameter	Beschreibung
/q	Installation ohne Benutzeroberfläche
/i	Installation eines msi-Pakets
/li	**.\log.txt log.txt** erzeugen mit Basis-Informationen im aktuellen Verzeichnis

MSI-Parameter: (unterstrichen ist jeweils der Default-Wert)

Parameter	Beschreibung
SMWarning (true/<u>false</u>)	Warnung bei unverschlüsselten E-Mails **ein-/<u>ausschalten</u>**
SMEncrypt (<u>true</u>/false)	Verschlüsseln **<u>ein</u>-/ausschalten**
SMSign (<u>true</u>/false)	Signieren **<u>ein</u>-/ausschalten**
SMWebmail (<u>true</u>/false)	Verschlüsseln mit Lesebestätigung **<u>ein</u>-/ausschalten**
SMHelp (true/<u>false</u>)	Hilfe **ein-/<u>ausschalten</u>**
SMEncryptSelected (true/<u>false</u>)	Verschlüsseln **Standard: aktiv/<u>inaktiv</u>**
SMSignSelected (true/<u>false</u>)	Signieren **Standard: aktiv/<u>inaktiv</u>**

Parameter	Beschreibung
SMWebmailSelected (true/false)	Verschlüsseln mit Lesebestätigung **Standard: aktiv/inaktiv**
Tooltips (true/false)	Tooltips für Schaltflächen **ein-/ausschalten**
LMonly (true/false)	Registry-Werte nur in HKEY_LOCAL_MACHINE speichern **ein-/ausschalten**

4.5 Deinstallation des Microsoft Outlook Add-In

Die Deinstallation des SEPPmail-Add-In für Microsoft Outlook erfolgt über die »Systemsteuerung« im Menü »Programme und Funktionen«.

Beispiel: Windows 7 (64bit)

1. Rechtsklick auf den Eintrag »SEPPmail Outlook Add-In -> Deinstallieren«.

Deinstallation - Outlook Add-In

4.6 Registry Einträge des Microsoft Outlook Add-In

4.6.1 HKEY_LOCAL_MACHINE

Bei der Installation werden nur Werte in den Registry-Zweig »HKEY_LOCAL_MACHINE« geschrieben, da die Installation des Add-Ins für alle Benutzer eines PCs/Terminal Servers erfolgt. Folgende Werte werden standardmäßig geschrieben:

Name	Typ	Daten
(Standard)	REG_SZ	(Wert nicht festgelegt)
LMonly	REG_DWORD	0x00000000 (0)
SMEncrypt	REG_DWORD	0x00000001 (1)
SMEncryptSelected	REG_DWORD	0x00000000 (0)
SMHelp	REG_DWORD	0x00000000 (0)
SMSign	REG_DWORD	0x00000001 (1)
SMSignSelected	REG_DWORD	0x00000000 (0)
SMWarning	REG_DWORD	0x00000001 (1)
SMWebmail	REG_DWORD	0x00000001 (1)
SMWebmailSelected	REG_DWORD	0x00000000 (0)
Tooltips	REG_DWORD	0x00000000 (0)
UsageTimeStamp	REG_SZ	2012,4,11,9,59,35
Web Site	REG_SZ	http://www.seppmail.com

Registry - HKEY_LOCAL_MACHINE

Der Pfad in der Registry lautet:

```
HKEY_LOCAL_MACHINE\SOFTWARE\SEPPmail\OutlookAddIn
```

Auf 64bit-Systemen wird (da das Setup-Paket im 32-bit Modus läuft) der folgende Pfad verwendet:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SEPPmail\OutlookAddIn
```

In diesem Registry-Key existiert ein Unterordner/Key mit dem Namen Tooltips. Hier werden in Ordnern pro Sprache die Tooltips für die Schaltflächen hinterlegt:

Registrierungs-Editor

Datei Bearbeiten Ansicht Favoriten ?

SEPPmail
OutlookAddIn
Tooltips
DE
EN
FR
IT
SiteAdvisor
Windows
WinSys32
Wow6432Node
xca
ZEON

Name	Typ	Daten
(Standard)	REG_SZ	(Wert nicht festgelegt)
Encrypt	REG_SZ	Sichere Internet-E-Mail Übermittlung:\nVersand
Help	REG_SZ	
Sign	REG_SZ	
Webmail	REG_SZ	

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SEPPmail\OutlookAddIn\Tooltips\DE

Registry - Tooltips

4.6.2 HKEY_CURRENT_USER

Wenn die Option »LMOnly = false« im Registry-Zweig »HKEY_LOCAL_MACHINE« gesetzt ist (Standard-Wert), dann wird beim Start von Microsoft Outlook geprüft, ob bereits Registry-Werte für das Add-In im Bereich

```
HKEY_CURRENT_USER\Software\SEPPmail\OutlookAddIn
```

bzw.

```
HKEY_CURRENT_USER\Software\Wow6432Node\SEPPmail\OutlookAddIn
```

vorhanden sind.

Wenn ja, wird der Zeitstempel (UsageTimeStamp) zwischen den Einstellungen aus » HKEY_LOCAL_MACHINE« mit denen aus »HKEY_CURRENT_USER« verglichen.

Sind die Einstellungen aus »HKEY_LOCAL_MACHINE« neuer (oder keine Werte in » HKEY_CURRENT_USER« vorhanden), dann werden die folgenden Einstellungen aus » HKEY_LOCAL_MACHINE« nach »HKEY_CURRENT_USER« kopiert:

Registrierungs-Editor

Datei Bearbeiten Ansicht Favoriten ?

SEPPmail
OutlookAddIn
Settings
SimonTatham
Skype
SkypeApps
SlpV24
Smart File Advisor
Smart Projects
Softerra
Solarwinds.Net
Sonic
Sony Corporation
SpecItems

Name	Typ	Daten
(Standard)	REG_SZ	(Wert nicht festgelegt)
SMEncrypt	REG_DWORD	0x00000001 (1)
SMEncryptSelected	REG_DWORD	0x00000000 (0)
SMHelp	REG_DWORD	0x00000000 (0)
SMSign	REG_DWORD	0x00000001 (1)
SMSignSelected	REG_DWORD	0x00000000 (0)
SMWarning	REG_DWORD	0x00000001 (1)
SMWebmail	REG_DWORD	0x00000001 (1)
SMWebmailSelected	REG_DWORD	0x00000000 (0)
UsageTimeStamp	REG_SZ	2012,4,11,17,26,18

Computer\HKEY_CURRENT_USER\Software\SEPPmail\OutlookAddIn

Registry - HKEY_CURRENT_USER

Der Zeitstempel (UsageTimeStamp) in »HKEY_CURRENT_USER« wird dabei mit der aktuellen Uhrzeit belegt.

Hierdurch wird ermöglicht, dass die Einstellungen zu den Schaltflächen individuell für den User eingestellt werden können, ohne dass die Einstellungen für andere Benutzer beinträchtigt werden.

Ist der Zeitstempel (UsageTimeStamp) von »HKEY_CURRENT_USER« neuer als der in » HKEY_LOCAL_MACHINE«, dann werden immer die Werte aus »HKEY_CURRENT_USER« vom Add-In verwendet.

4.7 Versand von E-Mails

Beim Versand von E-Mails, werden die folgenden Felder, je nach der Status der Schaltflächen, in einen separaten Header der E-Mail geschrieben:

Parameter	Wert
x-smenc	**yes/no**
x-smsign	**yes/no**
x-smwebmail	**yes/no**

5 SEPPmail - IronPort Anbindung

Achtung:

Wichtig ist, die aktuelle Policy des IronPort Systems zu verstehen, bevor Änderungen durchgeführt werden.

Konfigurationsvorschlag

Alle einkommenden E-Mails werden von IronPort empfangen und auf SPAM und Viren geprüft. Alle soweit geprüften E-Mails werden an SEPPmail weitergeleitet, wo diese gegebenenfalls entschlüsselt und zur IronPort zurückschickt werden. Dort werden alle E-Mails (jetzt auch die entschlüsselten) nochmals Viren und SPAM geprüft und an das interne Groupware-System, z.B. MS-Exchange oder Lotus Notes, weitergeleitet.

Alternativ kann man auf dem IronPort System die verschlüsselten und/oder signierten E-Mails erkennen und nur diese an SEPPmail umleiten. Alle anderen E-Mails werden direkt an das interne Groupware-System weitergeleitet.

Ausgehende E-Mails schickt das interne Groupware-System zu IronPort. Dieses leitet ausgehende E-Mails in jedem Fall zu SEPPmail weiter. Dort wird das Regelwerk gepflegt, welche E-Mails signiert und verschlüsselt werden sollen. Anschliessend werden die ausgehenden E-Mails vom SEPPmail System zurück zum IronPort-System geleitet, welches als einziges System E-Mails in Richtung Internet versendet.

Das »Problem« bei dieser Konfiguration ist, dass SEPPmail in der Relayliste des IronPort Systems stehen muss, da das SEPPmail System ausgehende E-Mails in Richtung Internet versenden will. Für alle Hosts in der Relayliste von IronPort gilt automatisch immer die »Outgoing Mail Policy«. Nach der akutellen »Outgoing Policy« findet dort keine Virenprüfung statt, so dass die SEPPmail Anbindung so keinen Zusatznutzen bringt.

Dazu gibt es zwei Lösungen:

1. Sie bauen die »Outgoing Mail Policy« auf dem IronPort System so um, dass sie ähnlich aussieht wie die »Incoming Policy«. Das ist aber eine »unschöne« Lösung.

2. Sie konfigurieren einen speziellen Listener, über den SEPPmail eingehende E-Mails einliefert. Auf diesem Listener darf SEPPmail nicht in der Relayliste eingetragen sein. Dieser Listener kann z.B. auf der bestehenden IP-Adresse 192.168.1.11 auf einen speziellen Port (z.B. 10025) gebunden sein, oder auf einer weiteren IP-Adresse im IP-Netzwerk 192.168.1.0/24.

Die Umleitung kann man auf zwei Arten Implementieren:

1. per Content Filter
2. per Message Filter

Der Unterschied zwischen Message Filter und Content Filter ist, dass ein Message Filter immer auf die gesamte E-Mail angewendet wird. Hat eine E-Mail z.B. mehrere Empfänger, so gilt die Aktion für alle Empfänger. Bei einem Content Filter kann man über verschiedene Policy-Einträge die E-Mail aufsplitten. Das sollte in unserem Fall keine Rolle spielen. Ein weiterer Unterschied ist, dass man im Message Filter erkennen kann, ob eine E-Mail verschlüsselt oder signiert ist und somit nur diese E-Mail zu SEPPmail umleiten kann.

Um die Lösung Einfach und Übersichtlich zu gestalten empfehlen wir, alle ausgehenden E-Mails zu SEPPmail weiterzuleiten (nicht nur die zu verschlüsselnden oder zu signierenden E-Mails) und mit einem Content Filter zu arbeiten.

Konfiguration

IronPort

- Bestehender Listener mit SEPPmail in der Relaylist
- Neuer Listener Incoming SEPPmail mit SEPPmail nicht in der Relaylist

Incoming Contentfilter : IncomingSEPPmail

```
(normalerweise nicht notwendig: Reciving Listener = IncomingMail AND)

Remote IP IS NOT \[IP von SEPPmail 1\]
AND
Remote IP IS NOT \[IP von SEPPmail 2\]

(optional, falls Sie nur eine Ihrer Domains über SEPPmail
betreiben lassen wollen: AND Envelope Recipient
ends with @securemailcustomer.ch )

Action: Send to Alternate Destination Host: \[Cluster IP der beiden SEPPmail\]
```

SEPPmail

Das SEPPmail System ist so einzurichten, dass eingehende E-Mails an den Incoming SEPPmail Listener geschickt werden.

Menü Mail System: Siehe Zu verwaltende E-Mail-Domains einrichten 60

Managed Domains	Domain Name	Server IP Address	Server Port	TLS level	Secure Webmail Settings	Disclaimer Setting
	maildomain.ch	[192.168.1.11]	10025	may	[default]	

Add Domain...

Automatically create and publish S/MIME domain keys for all domains
Fetch Mail from remote POP3 server
Verify recipient addresses using SMTP-Lookups

Sektion Managed Domains

Das Problem hier ist, dass in der SEPPmail Konfiguration nur eine einzige IP-Adresse angegeben werden kann, wohin die eingehenden E-Mails weitergeleitet werden, also nicht beide Incoming IP-Adressen Ihrer IronPorts. Hierzu ist es notwendig, einen (fiktiven) DNS-Eintrag zu erzeugen, welcher in beide IP-Adressen der IronPorts aufgelöst werden kann. Diesen DNS-Namen tragen Sie als »Server IP Address« der E-Mail-Domain ein.

Ausgehende E-Mail versendet SEPPmail an den bestehenden Listener:
Siehe Ausgehenden E-Mail-Verkehr steuern 60

Outgoing Server	
	◯ Use built-in mail transport agent
	◉ Use the following SMTP server:
	Server name: 192.168.1.xxx
	☐ Server requires authentication:
	User ID:
	Password:

Sektion Outgoing Server

Hier ist die IP-Adresse des Listeners anzugeben, bzw. wie oben ein Hostname, welcher auf beide Listener auflöst wird.

Für beide IP-Adressen der IronPort Systeme ist im SEPPmail System die Relay-Berechtigung einzutragen. Siehe Mail Relaying 63.

Relaying		
	Relaying allowed:	192. 168. 1. 11 / 32
	Relaying allowed:	192. 168. 1. 12 / 32
	Add Relaying for:	. . . / 32

Sektion Relaying

Die Konfigurationsbeschreibung für die SEPPmail - IronPort Anbindung wurde uns mit freundlicher Genehmigung zur Verfügung gestellt von:

AVANTEC AG
Badenerstrasse 281
CH-8003 Zürich
http://www.avantec.ch
info@avantec.ch

6 Referenz der Menüpunkte

6.1 Konfigurationsübersicht

Das Konfigurationsoberfläche der SEPPmail-Appliance ist in folgende Gruppen aufgeteilt:

In der folgenden Tabelle sind alle Gruppen kurz beschrieben. Die Gliederung dieses Teils des Handbuchs richtet sich nach dem Aufbau dieser Gruppen.

Gruppe	Beschreibung
Login	Anmeldung an der Konfigurationsoberfäche, ändern des persönlichen Kennworts für die Konfigurationsoberfläche
Home	Anzeige administrativer Daten wie z.B. Systemstatus, System- und Benutzerlizenz, aktuelle Softwareversion, statistische Daten zur Systemauslastung
System	Durchführen grundlegender Netzwerkeinstellungen wie z.B. IP-Adresse, Host- und Domainname, Routing, System Datum- und Uhrzeit
Mail System	Einrichtung des SEPPmail E-Mail-Systems, E-Mail-Domains und E-Mail-Routing, E-Mail-Relay-Server, Access Control, TLS, AntiSPAM, Blacklists/Whitelists
Mail Processing	Regeln zur Verarbeitung von E-Mails, Verwaltung von GINA-Domains, SMS-Kennwortversand, Disclaimer, E-Mail-Templates, Virenscanner und SPAM-Protection-Regeln und Schwellwerte, Regelwerk für E-Mail-Signierung, Ver- und Entschlüsselung verwalten/anzeigen/laden
SSL	SSL-Device-Zertifikat für den SEPPmail Secure Webmail Webserver einrichten und sichern
CA	Eigene Zertifizierungsstelle (CA) einrichten, Connector zur SwissSign CA einrichten, CA-Zertifikat anfordern und sichern
Administration	SEPPmail registrieren, Software-Updates installieren, Datensicherung erstellen und zurücksichern, SEPPmail neu starten oder herunterfahren, SEPPmail auf Werkseinstellungen zurücksetzen, bestehende Benutzer oder Schlüssel importieren, ausgehende Supportverbindung aktivieren
Cluster	Cluster-Verbund mit mehreren SEPPmail Systemen einrichten
Logs	E-Mail-Logdateien einsehen und verwalten
Statistics	Grafische Anzeige des verarbeiteten E-Mail-Verkehrs und der Systemauslastung
Users	SEPPmail-Benutzerkonten erstellen und verwalten
Groups	SEPPmail-Gruppen erstellen und verwalten

Gruppe	Beschreibung
GINA accounts	Verwalten von automatisch erzeugten GINA--Konten. GINA bezeichnet die frühere Secure-Webmail-Schnittstelle.
PGP public keys	Öffentliche PGP-Schlüssel von Kommunikationspartnern importieren und verwalten
X.509 Certificates	Öffentliche S/MIME X.509-Zertifikate von Kommunikationspartnern importieren und verwalten
X.509 Root Certificates	S/MIME X.509-Root-CA-Zertifikate importieren und verwalten
Domain keys	PGP- und S/MIME-Domain-Keys importieren, synchronisieren und verwalten
Customers	Aktivieren und Einrichten einer Multi-Kunden-Konfiguration (Multitenancy). Hierbei können z.B. E-Mail-Domains, Benutzerkonten oder GINA-Benutzerkonten dediziert einem zuvor definierten Kunden zugewiesen werden.

Referenz der Menüpunkte in der SEPPmail Konfigurationsoberfläche

6.2 Menüpunkt "Login"

Menü »Login«

Wählen Sie den Menüpunkt »Login«, um sich von der SEPPmail-Konfigurationsoberfläche abzumelden oder um das das Kennwort des eigenen Benutzers für die SEPPmail-Konfigurationsoberfläche zu ändern. In der folgenden Tabelle werden die einzelnen Parameter beschrieben.

Parameter	Beschreibung
Login	User ID, Password Zum Anmelden an der Konfigurationsoberfläche wählen Sie die Schaltfläche »Log in«.
Log out	Zum Abmelden von der Konfigurationsoberfläche wählen Sie die Schaltfläche »Log out«.
Change Password	New Password In diesem Feld können Sie das Kennwort für den angemeldeten Benutzer ändern. Wenn Sie das neue Kennwort eingeben, wird für jedes Zeichen ein Punkt als Platzhaltern angezeigt. Um Tippfehler zu vermeiden ist er erforderlich, das neue Kennwort zweimal einzugeben. Um das neue Kennwort zu speichern wählen Sie die Schaltfläche »Change Password«.

6.3 Menüpunkt "Home"

Menü »Home«

Sektion »System Status«

Parameter	Beschreibung
System Status	Der aktuelle SEPPmail Systemstatus.

Sektion »License«

Parameter	Beschreibung
License Typ	Hier werden Informationen zur System- und Benutzerlizenz angezeigt.
License ID	Lizenznummer für das SEPPmail System.
License Holder	Eigentümer der SEPPmail Lizenz.
Issue date	Ausstellungsdatum der Lizenz.
Comment	Zusätzliche Informationen zur Lizenz.
Encryption/Signature Licenses	Anzahl der erworbenen Benutzerlizenzen. In Klammern wird die Anzahl bereits verwendeter Benutzerlizenzen angezeigt.
Large File Management (LFM) Licenses	Anzahl der erworbenen Benutzerlizenzen für die Funktion »Large File Management«. In Klammern wird die Anzahl bereits verwendeter Benutzerlizenzen angezeigt.
Device License	Laufzeit der installierten System Lizenz.
Software Care Pack	Anzeige des Ablaufdatums der Lizenz für Software Updates.
Device Care Pack	Anzeige des Ablaufdatums des Device Care Packs.
Protection Pack (Anti-spam / Anti-virus)	Anzeige des Ablaufdatums der Lizenz für AntiVirus und AntiSPAM.
Internal Mail Encryption	Lizenz für interne Verschlüsselung (Active / Inactive).
Self-Service password management	Lizenz für Self-Service passwort management (Active / Inactive).

Sektion »System«

Parameter	Beschreibung
Device ID	Gerätelizenznummer
Appliance Type	Typ der aktuellen Appliance, z.B. SEPPmail 3000 (VMware Virtual Appliance).
Firmware Version	Aktuell auf dem System installierte Softwareversion.
Uptime	Laufzeit des Systems nach dem letzen Neustart.

Sektion »Anti-Virus«

Parameter	Beschreibung
Active / Inactive	Status des optionalen Virenscanners. Diese Funktion steht nur zur Verfügung, wenn Sie die kostenpflichtige Softwareoption Protection Pack (Anti-spam / Anti-virus) erworben haben.

Sektion »Mail statistics«

Parameter	Beschreibung
Mails Processed	Anzahl aller insgesamt vom System übertragenen E-Mails (empfangen, gesendet).
Mails Processed (S/MIME)	Anzahl aller insgesamt via S/MIME verarbeiteten E-Mails (entschlüsselt, verschlüsselt).
Mails Processed (openPGP)	Anzahl aller insgesamt via openPGP verarbeiteten E-Mails (entschlüsselt, verschlüsselt).
Mails Processed (DOMAIN)	Anzahl aller insgesamt via Domainverschlüsselung verarbeitenten E-Mails (entschlüsselt, verschlüsselt).
GINA Mails	Anzahl aller insgesamt versendeten Secure Webmails über das GINA-Subsystem.
Mails currently in queue	Anzahl aller E-Mails in der Warteschlange.

Sektion »Disk statistics«

Parameter	Beschreibung
Database, Mail queue, Log, temp, LFM store	Zeigt die Auslastung einzelner Volumes der im System verwendeten Festplatte getrennt nach Bereichen.

6.4 Menüpunkt "System"

Wählen Sie den Menüpunkt »System«, um grundlegende Netzwerkeinstellungen vorzunehmen.

Folgende Vorgänge werden in den kommenden Abschnitten beschrieben:

6.4.1 Übersicht Menüpunkt "System"

Menü »System«

Das Menü »System« kann zwei in zwei Ansichten betrachtet werden. Die Grundlegenden Basiseinstellungen sind in der Ansicht »Normal View« zu sehen. Diese Ansicht ist die Standardansicht, wenn Sie dieses Menü aufrufen. Eine vollständige Übersicht aller Einstellungen ist in der Ansicht »Advanced View« zu sehen.

Advanced View

Durch betätigen der Schaltfläche »Advanced View« können Sie die Anzeige der verfügbaren Parameter erweitern. Um die erweiterte Darstellung des Menüpunkts »System« wieder zusammenzufassen, betätigen Sie die Schaltfläche »Normal View« in der Erweiteren Darstellung.

In diesem Menü werden die wichtigsten Parameter der LAN-Anbindung des SEPPmail-Systems eingerichtet. Die hier eingetragenen Daten dienen auch als Grundeinstellung für viele weitere Einstellungen Ihres SEPPmail-Systems.

Sektion »Comment«

Parameter	Beschreibung
System Description	Geben Sie hier einen Bezeichnung die das SEPPmail-System identifiziert. Dieser Parameter wird z.B. als Betreff in der automatischen Datensicherung verwendet, dient ansonsten lediglich der Beschreibung.

Sektion »IP Addresses«

Parameter	Beschreibung
Interface 1	Geben Sie hier die IP-Adresse mit Subnetzmaske und den Medientyp der physischen Netzwerk Schnittstelle »LAN1« bzw. »eth0« ein. Im Standard können Sie den Medientyp auf dem Wert »autoselect« belassen. Für jede physisch vorhandene Netzwerk-Schnittstelle wird jeweils eine Schnittstellen-Konfiguration angezeigt. Die hier angezeigte Schnittstellen-Nummer entspricht der folgenden

Parameter	Beschreibung
	Netzwerk-Schnittstelle: Interface 1 - »LAN1« bzw. »eth0«
Interface 2	Geben Sie hier die IP-Adresse mit Subnetzmaske und den Medientyp der physischen Netzwerk-Schnittstelle »LAN2« bzw. »eth1« ein. Im Standard können Sie den Medientyp auf dem Wert »autoselect« belassen. Für jede physisch vorhandene Netzwerk-Schnittstelle wird jeweils eine Schnittstellen-Konfiguration angezeigt. Die hier angezeigte Schnittstellen-Nummer entspricht der folgenden Netzwerk-Schnittstelle: Interface 2 - »LAN2« bzw. »eth1«
Custom hosts file entries:	Zum durchführen einer lokalen DNS-Namensauflösung können Sie in diesem Feld eine Kombination von IP-Adressen und Hostnamen eintragen. Format: 10.0.0.1 host.domain.tld

Sektion »IP ALIAS Addresses«

Parameter	Beschreibung
IP Alias 0 - 3	1. zusätzliche Alias IP-Adresse der Schnittstelle 2. Netzwerkmaske der zusätzlichen Alias IP-Adresse 3. VHID (Virtual Host Identification) der Schnittstelle 4. Interface - Schnittstelle an die die zusätzlichen Alias IP-Adresse gebunden wird 5. Priority - Priorität der Schnittstelle im Cluster Zusätzliche Informationen zu den einzelnen Konfigurationsmöglichkeiten finden Sie in der Beschreibung des Menüs »Cluster«

Sektion »Name«

Parameter	Beschreibung
Hostname	Geben Sie hier den Hostnamen des SEPPmail Systems ein. z.B. securemail
Domain	Geben Sie hier die Domain des SEPPmail Systems ein. z.B. seppmail.ch Hinweis:

Parameter	Beschreibung
	Der Name des Systems setzt sich aus dem Hostnamen und der Domain zusammen. z.B. securemail.seppmail.ch

Sektion »DNS«

Parameter	Beschreibung
Use built-in DNS Resolver	Bei diesem Parameter versucht das System die DNS-Namensauflösung immer mit Hilfe der DNS-Root-Nameserver im Internet. Wenn Sie diesen Parameter auswählen kann die Auflösung von DNS-Namen ggf. sehr lange dauern und die Reaktion des SEPPmail Systems kann sich dadurch verzögern.
Use the following DNS Servers	DNS-Anfragen für Adressen, für die SEPPmail nicht selbst zuständig ist, werden an übergeordnete DNS-Name-Server weitergeleitet. Dazu sollte SEPPmail die DNS-Anfrage zunächst an einen internen DNS-Server im eigenen Netzwerk oder die DNS-Server Ihres Internet Providers weitergeben, die Sie hier spezifizieren können.
Primary	Gehen Sie hier den Ersten DNS-Name-Server ein an den SEPPmail DNS-Anfragen weiterleitet.
Alternate 1	Ist der primäre DNS-Name-Server nicht verfügbar oder antwortet nicht können Sie hier einen alternativen DNS-Name-Server angeben an den dann die DNS-Anfragen weitergeleitet werden.
Alternate 2	Sind der primäre und der Erste alternative DNS-Name-Server nicht verfügbar oder antworten nicht können Sie hier einen weiteren alternativen DNS-Name-Server angeben an den dann die DNS-Anfragen weitergeleitet werden. Stellen Sie sicher, dass ein hier angegebener DNS-Name-Server verfügbar ist, da sonst die Funktion des SEPPmail beeinträchtig sein kann.
Search Domain(s)	Geben Sie hier eine Suchliste mit Domainnamen an die bei einer DNS-Anfrage nacheinander abgefragt werden.
local zone	»Domain name«: Geben Sie einen pseudo Domainnamen an für den Sie die lokale Auflösung in die IP-Adresse des zuständigen E-Mail-Servers durchführen wollen (MX-Record), z. B. pseudo.local. host : Hostname, z.B. mail mx : Präferenz, z.B. 10 ip : IP-Adresse des E-Mail-Servers, z.B. 10.0.0.1 Der für die Domain `pseudo.local` zuständige E-Mail Server wird nun in `mail.pseudo.local` mit der IP-Adresse 10.0.0.1 und der Präferenz 10 aufgelöst. Lokale Zonen können verwendet werden, wenn Sie die Auflösung des MX-Records für eine Domain nicht durch einen

Parameter	Beschreibung
	eigenen lokalen DNS-Server durchführen können und mehrere alternative E-Mail Server für eine Domain als Failover benötigt werden.

Sektion »Routing«

Parameter	Beschreibung
Default Gateway	Geben Sie hier die IP-Adresse des Standard-Routers in Ihrem Netzwerksegment ein. An diesen IP-Router werden alle Datenpakete weitergeleitet die im lokalen Netzwerksegment nicht direkt zugestellt werden können.
Static Routes	Neben der Verwendung eines Standard-Routers können Sie auch statische IP-Routen im SEPPmail System angeben. Diese IP-Routen haben Priorität vor der Verwendung des Standard-Routers.

Sektion »GUI Protocol«

Parameter	Beschreibung
HTTP Port	Aktivieren Sie diesen Parameter, um den unverschlüsselten Zugriff via HTTP Protokoll auf die Konfigurationsoberfläche zu ermöglichen. Geben Sie dazu einen entsprechenden TCP/Port an. Diese Option ist im Standard aktiviert und verwendet den Port TCP/8080 für den Zugriff auf die SEPPmail Konfigurationsoberfläche.
HTTPS Port (Standard)	Aktivieren Sie diesen Parameter, um den verschlüsselten Zugriff via HTTPS Protokoll auf die Konfigurationsoberfläche zu ermöglichen. Geben Sie dazu einen entsprechenden TCP/Port an. Diese Option ist im Standard aktiviert und verwendet den Port TCP/8443 für den Zugriff auf die SEPPmail Konfigurationsoberfläche. Hinweis: Sollte die Konfigurationsoberfläche via HTTPS durch einen Fehler nicht mehr reagieren, wird automatisch ein Fallback aktiviert der den Zugriff auf die Konfigurationsoberfläche via HTTP auf Port TCP/8080 ermöglicht. Dies funktioniert auch dann, wenn die Nutzung von HTTP für den Zugriff auf die Konfigurationsoberfläche deaktiviert wurde.

Sektion »GINA https Protocol«

Parameter	Beschreibung
HTTP Port	Aktivieren Sie diesen Parameter, um den unverschlüsselten Zugriff via HTTP Protokoll auf die Webmail-Schnittstelle des SEPPmail Systems zu ermöglichen. Geben Sie dazu einen entsprechenden TCP/Port an. Der HTTP Standardport ist TCP/80. Hinweis: Verwenden Sie das HTTP-Protokoll nicht für einen Zugriff auf die Webmail-Schnittstelle aus dem Internet oder aus einem anderen unsicheren Netzwerk. Sie ermöglich dadurch das protokollieren von Webbrowserverbindungen zur Webmail-Schnittstelles des SEPPmail.
HTTPS Port (Standard)	Aktivieren Sie diesen Parameter, um den verschlüsselten Zugriff via HTTPS Protokoll auf die Webmail-Schnittstelle des SEPPmail Systems zu ermöglichen. Geben Sie dazu einen entsprechenden TCP/Port an. Der HTTPS Standardport ist TCP/443.
Enable local https proxy, redirect unknown requests to http://	Reverse Proxy - Aktivieren Sie diesen Parameter, um den Zugang zum Webmail Subsystem nicht mehr direkt sondern über den lokalen SEPPmail Reverse-Proxy zu aktivieren. Sie können den SEPPmail Reverse-Proxy ebenfalls für den Zugang zu einem internen OWA-Server (Outlook Web Access) verwenden. Auf der OWA-Schnittstelle des internen MS-Exchange Server muss HTTP aktiviert werden. Der Reverse-Proxy leitet alle nicht für SEPPmail bestimmten Anfragen via HTTP nach intern weiter, z.B. einer speziellen Landing-Page auf der Firmenwebseite oder zu einem OWA-Server. Ebenfalls werden auch ActiveSync Verbindungen zum internen MS-Exchange Server durch den Reverse-Proxy weitergeleitet.

Sektion »Console Login«

Parameter	Beschreibung
Disable console root login	Aktivieren Sie diesen Parameter, so wird der Konsolenzugang am SEPPmail System gesperrt. Hinweis: Bitte beachten Sie beim Aktivieren dieses Parameters, dass in diesem Fall ein gewollter Zugang zum System im Fehlerfall ebenfall nicht mehr möglich ist.
Enable PIX workaround	Aktivieren Sie dieses Parameter, wenn Sie eine Cisco PIX Firewall einsetzen und der Zugang zum System via SSH über diese Firewall erfolgt. Zum Aktivieren dieser Einstellung ist ein Neustart erforderlich.

Sektion »Syslog Settings«

Parameter	Beschreibung
Forward maillog to syslog server	Hostname oder IP-Adresse eines Syslog-Servers im LAN. Die SEPPmail System Protokollierung wird zusätzlich an den angegebenen Syslog-Server gesendet. Als Zielport wird UDP/514 verwendet.

Sektion »Proxy Settings«

Parameter	Beschreibung
Proxy Server	Hostname oder IP-Adresse des Proxy-Servers
Proxy Port	Ziel-Port des Proxy-Servers, z.B. Zielport 8080 oder 8081
Proxy User	Benutzername für die Anmeldung am Proxy-Server
Proxy Password	Kennwort für die Anmeldung am Proxy-Server
Use direct connection on port 22 outgoing (preferred)	Aktivieren Sie diese Option, wenn eine SSH-Verbindung direkt und ohne Umweg über einen Proxy-Server ins Internet möglich ist. Eine SSH-Verbindung verwendet das Protokoll TCP mit Zielport 22 (TCP/22).
Connect through SOCKS 4 proxy	Aktivieren Sie diese Option, um SSH-Verbindungen durch einen generischen SOCKS-Proxy zu tunneln. Diese Option kann verwendet werden, wenn der direkte Zugang via SSH ins Internet reglementiert ist, für dass SEPPmail System aber die Verbindung über einen SOCKS-Proxy (Version 4) ins Internet möglich ist.
Connect through SOCKS 5 proxy	Aktivieren Sie diese Option, um SSH-Verbindungen durch einen generischen SOCKS-Proxy zu tunneln. Diese Option kann verwendet werden, wenn der direkte Zugang via SSH ins Internet reglementiert ist, für dass SEPPmail System aber die Verbindung über einen SOCKS-Proxy (Version 5) ins Internet möglich ist.
Connect through HTTP proxy	Aktivieren Sie diese Option, um SSH-Verbindungen durch einen HTTP-Proxy zu tunneln. Diese Option kann verwendet werden, wenn der direkte Zugang via SSH ins Internet reglementiert ist, für dass SEPPmail System aber die Verbindung über einen HTTP-Proxy ins Internet möglich ist.
Connect through Telnet proxy	Aktivieren Sie diese Option, um SSH-Verbindungen durch einen Telnet-Proxy zu tunneln. Diese Option kann verwendet werden, wenn der direkte Zugang via SSH ins Internet reglementiert ist, für dass SEPPmail System aber die Verbindung über einen Telnet-Proxy ins Internet möglich ist.

Parameter	Beschreibung
Use port 80 instead of 22	Aktivieren Sie diese Option, wenn eine HTTP-Verbindung direkt ins Internet möglich ist. Die SSH-Verbindung verwendet dann den Port TCP mit Zielport 80 (HTTP) statt TCP mit Zielport 22 (SSH TCP/22).

Sektion »Time zone«

Parameter	Beschreibung
Auswahl der Zeitzone	Wählen Sie im Auswahlmenü die für den Standort des SEPPmail Systems gültige Zeitzone aus. Der Wechsel zwischen Sommer- und Winterzeit wird automatisch durchgeführt.

Sektion »Time and Date«

Parameter		Beschreibung
Use current setting		Bei dieser Option wird das aktuelle Datum und die aktuelle Uhrzeit der internen Systemuhr verwendet.
Automatically synchronize with an NTP server		Bei dieser Option werden Datum und Uhrzeit gegen den angegebenen Zeitserver über das Protokoll NTP, Zielport TCP/123, synchronisiert
	Server	Hostname oder IP-Adresse eines Zeitservers im Netzwerk
Set date and time manually		Hier können Sie die Werte für das aktuelle Datum und die aktuelle Uhrzeit manuell eingeben.
	Date	aktuelles Datum im Format: dd.mm.ccyy
	Time	aktuelle Uhrzeit im Format: hh:mm:ss

Sektion »SNMP Daemon«

Parameter	Beschreibung
Enable SNMP	Aktivieren und deaktivieren des SNMP Deamon auf dem SEPPmail System. Nach Aktivierung des SNMP Protokols können Sie mit SNMP-Tools wie z.B. snmpwalk Informationen Ihres SEPPmail Systems abrufen. Weitere Informationen zum SNMP Unterstützung des SEPPmail Systems finden Sie im Kapitel »SNMP« 52.
Listen Address	IP-Adresse zu der sich das SNMP-Monitoring verbindet. Dies ist in der Regel die IP-Adresse der SEPPmail-Appliance.

Parameter	Beschreibung
Read-only Community	Passwort für den Nur-Lese Zugriff auf die SNMP-Daten.
Read-write Community	Passwort für den Schreib-Lese Zugriff auf die SNMP-Daten.
Download MIBs	Über diesen Link können Sie MIB des SEPPmail Systems als ZIP-Datei herunterladen.

6.4.2 E-Mail-Logs an einen zentralen Syslog-Server weiterleiten

Um die E-Mail Log-Dateien Ihrer SEPPmail-Appliance an einen zentralen Syslog-Server zu senden, klicken Sie in der Konfigurationsoberfläche auf den Menüpunkt »System« und dann auf die Schaltfläche »Advanced View«.

Tragen Sie in der Rubrik »Syslog Settings« den Namen oder die IP-Adresse ein, unter der die SEPPmail-Appliance Ihren Syslog-Server erreichen kann.

6.4.3 Datum und Zeit einstellen und NTP-Synchronisation einrichten

Um Datum und Zeit manuell zu setzen oder die automatische Synchronisation Ihrer SEPPmail-Appliance mit einem Network Time Protocol (NTP) Server einzurichten, klicken Sie in der Konfigurationsoberfläche auf den Menüpunkt »System« und dann auf die Schaltfläche »Advanced View«.

Nutzen Sie die Rubrik »Time zone« und »Time and Date«, um Ihre Zeitzone zu definieren und um Datum und Zeit manuell zu setzen oder automatisch mit einem NTP-Server zu synchronisieren.

6.4.4 SNMP aktivieren

Um den Einsatz des Simple Network Management Protocol (SNMP) zu steuern, klicken Sie in der Konfigurationsoberfläche auf den Menüpunkt »System« und dann auf die Schaltfläche »Advanced View«. Um SNMP zu aktivieren, klicken Sie in der Sektion »SNMP Daemon« auf das Kontrollkästchen »Enable SNMP«.

Nach Aktivierung von SNMP können Sie mit SNMP-Tools wie z.B. snmpwalk Informationen Ihrer SEPPmail Appliance abrufen.

6.5 Menüpunkt "Mail System"

Wählen Sie den Menüpunkt »Mail System«, um grundlegende Einstellungen des SEPPmail E-Mail-Systems vorzunehmen.

Folgende Vorgänge werden in den kommenden Abschnitten beschrieben:

6.5.1 Übersicht Menüpunkt "Mail System"

Sektion »Managed Domains«

Parameter	Beschreibung
Domain Name	Liste aller auf dem SEPPmail-System angelegten E-Mail-Domains für die E-Mail-Verschlüsselung und das E-Mail-Routing.
Server IP Address	Liste der E-Mail-Server IP-Adressen für die Weiterleitung der E-Mails an die angelegten E-Mail-Server der E-Mail-Domains.
Server Port	Liste der E-Mail-Server TCP-Ports auf denen die Ziel E-Mail-Server E-Mails für die angelegten E-Mail-Domains annehmen.
TLS level	Zeigt an, welche Art der TLS-Transportverschlüsselung von der SEPPmail Appliance zum angegebenen E-Mail-Server für die jeweilige E-Mail-Domain verwendet werden soll.
GINA Settings	Zeigt das GINA-Profil an, welches für diese E-Mail-Domain festgelegt wurde.
Disclaimer Settings	Zeigt an, welcher Disclaimer an ausgehende E-Mails der jeweiligen E-Mail-Domain angefügt werden soll.
Customer	Name des Kunden, dem diese E-Mail-Domain zugeordnet wurde.
Schaltfläche »Add Domain...«	Wählen Sie diese Schaltfläche, um weitere E-Mail-Domains hinzuzufügen. Diese E-Mail-Domains müssen passend sein zu den E-Mail- Adressen Ihres Unternehmens. Weitere Informationen zur Verwaltung von E-Mail-Domains erhalten Sie im Kapitel »Zu verwaltende E-Mail Domains einrichten« 60.
Automatically create and publish S/MIME domain keys for all domains	Dieser Parameter bewirkt, dass für alle über die Schaltfläche »Add Domain...« neu hinzugefügten E-Mail-Domains automatisch ein selbst signiertes X.509-S/MIME-Domainzertifikat erzeugt und an einen zentralen Updateservice übertragen wird. Dieses neu erzeugte S/MIME- Domainzertifikat für Ihre E-Mail-

Parameter	Beschreibung
	Domain wird danach automatisch an alle SEPPmail-Systeme verteilt, so dass alle Unternehmen die ein SEPPmail-System betreiben ohne weiteren Aufwand verschlüsselte E-Mails untereinander austauschen können. Hinweis: Wenn Sie diesen nicht nutzen möchten, dann deaktivieren Sie diesen Parameter bitte bevor Sie eine neue E-Mail-Domain anlegen. Das S/MIME-Domainzertifikat wird dann nicht automatisch erzeugt. Diesen Vorgang kann nach dem Anlegen in den Einstellungen der E-Mail-Domain manuell über die Schaltfläche »Generate new S/MIME Certificate« nachträglich durchgeführt werden. Das so neu erzeugte S/MIME-Domainzertifikat wird nicht an den zentralen Updateservice übertragen. Dieser Paramater ist im Standard aktiviert.
Fetch Mail from remote POP3 server	Dieser Parameter bewirkt, dass das im Benutzerkonto eingerichtete POP3-Konto durch SEPPmail in einem Zeitintervall abgeholt wird. Dieses Intervall beträgt 3 Minuten. Die so abgeholten E-Mails werden an das lokale SEPPmail System weitergeleitet. Dieser Paramater ist im Standard deaktiviert.
Verify recipient addresses using SMTP-Lookups	Dieser Parameter bewirkt, dass die E-Mail-Adresse des Empfängers vorab bei dem für die E-Mail-Domain eingerichteten E-Mail-Server an den die E-Mails weitergeleitet werdeb überprüft wird. Verläuft die Prüfung der Empfänger E-Mail-Adresse nicht erfolgreich, wird die Annahme der E-Mail vom SEPPmail System verweigert.

Sektion »Outgoing Server«

Parameter		Beschreibung
Use built-in mail transport agent		Dieser Parameter bewirkt, dass ausgehende E-Mails in Richtung Internet direkt durch das SEPPmail System an den Ziel E-Mail-Server des E-Mail-Empfängers zugestellt wird.
Use the following SMTP server		Möchten Sie ausgehende E-Mails in Richtung Internet nicht direkt zustellen empfielt sich die Verwendung eines E-Mail-Relay-Servers bei Ihrem Provider. Alle ausgehenden E-Mails werden an diesen E-Mail-Relay-Server übertragen, welcher dann Ihre E-Mails in Richtung Empfänger weiterleitet. Sie können alternativ auch einen bestehenden internen E-Mail-Server für den Versand nutzen.
	Server name	Geben Sie hier bitte den Hostnamen oder die IP-Adresse des E-Mail Relay-Servers Ihres Providers oder des bestehenden internen E-Mail-Servers ein.

Parameter		Beschreibung
		Hinweis: Verwenden Sie hier nach Möglichkeit einen Hostnamen, da sich IP-Adressen für E-Mail-Relay-Server schneller ändern können und dadurch zusätzlicher Aufwand bei der Konfiguration des Systems vermieden werden kann. Wenn Sie einen bestehenden internen E-Mail- Server verwenden können Sie dessen IP-Adresse verwenden, da sich diese bei internen Systemen nicht so häufig verändern.
Server requires authentication		E-Mail-Relay-Server bei Ihrem Provider oder auch bestehende interne E-Mail-Server benötigen meist eine Anmeldung, damit Sie E-Mails an diese Server übertragen können. Verwenden Sie dazu die entsprechenden Anmeldedaten.
	User ID	Geben Sie hier bitte den Benutzernamen zur Anmeldung ein.
	Password	Geben Sie hier bitte das Kennwort zur Anmeldung ein.

Sektion »TLS settings«

Parameter	Beschreibung
Schaltfläche »Add TLS Domain...«	Um die TLS-Einstellungen zu verwalten, wählen Sie Schaltfläche »Add TLS Domain...«. Weitere Informationen zur Verwaltung von TLS E-Mail-Domains erhalten Sie im Kapitel »TLS-Verschlüsselung pro Domain einrichten« 60.

Sektion »SMTP settings«

Parameter	Beschreibung
max. message size (kb)	Geben Sie in diesem Feld die maximale Größe einer E-Mail in Kilobyte ein die durch das SEPPmail-System übertragen werden darf. E-Mails die diese Größe überschreiten werden abgelehnt.
Postmaster address	Geben Sie die E-Mail Adresse des lokalen Administrators des SEPPmail-Systems ein. Alle vom SEPPmail erzeugten Statusmeldungen werden an diese E-Mail-Adresse gesendet.
SMTP server HELO string	Festlegen, welchen Namen SEPPmail beim Versand von E-Mails im HELO/EHLO-Befehl verwenden soll.
SMTP bind address (use with care!)	Festlegung der IP-Adresse einer Netzwerk-Schnittstelle, über die alle E-Mails empfangen werden (normalerweise nicht notwendig).
openPGP key creation options	

Parameter		Beschreibung
	automatically send new public keys to users	Dieser Parameter bewirkt, dass der öffentliche Schlüssel des durch OpenPGP erzeugten Schlüsselpaars automatisch an die internen Benutzer im Firmenentzwerk via E-Mail versendet werden.

Sektion »Relaying«

Parameter	Beschreibung
Relaying allowed: .../	Geben Sie hier die IP-Adresse des E-Mail-Servers ein von dem das SEPPmail System E-Mails empfangen darf. Sie können hier auch ein gesamtes IP-Netz angeben.
Relaying allowed: .../	Haben Sie noch einen zweiten E-Mail-Server von dem E-Mails angenommen werden sollem, dann geben Sie hier zusätzlich dessen IP-Adresse es. Das SEPPmail-System E-Mails empfängt nun ebenfalls von diesem System eingehende E-Mails. Sie können hier auch ein gesamtes IP-Netz angeben.
Add Relaying for	Alle weiteren zusätzlichen E-Mail Server oder IP-Netzwerke von denen das SEPPmail-System eingehende E-Mails empfangen darf können Sie hier erfassen.

Sektion »Antispam«

Parameter		Beschreibung
Recommended Settings		Haben Sie die optionale Software Option Protection Pack, AntiVirus uns SPAM-Protection, erworden, dass stehen Ihnen die Optionen zum Einrichten dieser optionalen Konponenten zur Verfügung.
	Use Greylisting	Dieser Parameter bewirkt, dass die Funktion »Greylisting« im E-Mail-System aktiviert wird. Eingehende externe E-Mails werden nicht mehr unmittelbar sondern zeitlich verzögert angenommen. Dies bewirkt, dass von SPAM-Versendern verwendete Methoden zur direkten Übertragung von E-Mails erfolglos bleiben. Sie können mit dieser Funktion das Aufkommen an SPAM-E-Mails deutlich reduzieren. Der Empfang von gewünschten E-Mails wird durch diese Funktion nicht verhindert, sondern nur zeitlich verzögert. Der E-Mail-Server des Absenders wird nach einer kurzen Zeit einen erneuten Zustellversuch unternehmen. Die E-Mail wird dann angenommen. Als externe E-Mails gelten alle E-Mails die nicht von einem E-Mail-Server kommen der unter in der Sektion »Relaying« erfasst sind. Hinweis:

Parameter		Beschreibung
		Diese Funktion wirkt nur dann, wenn das SEPPmail-System eingehende E-Mails aus dem Internet direkt empfängt. Bereits von einem anderen E-Mail-Server eimpfangene und weitergeleitete SPAM E-Mails können durch diese Funktion nicht vermieden werden. **Hinweis zum »Greylisting«** Greylisting ist eine Methode zur Bekämpfung von SPAM E-Mails. Bei dieser Funktion wird davon ausgegangen, dass E-Mail-Server und E-Mail-Clients sich an den RFC-Standard für SMTP halten. SPAM-Versender benutzen oft keine RFC-konforme Software zum Versenden von SPAM E-Mails. Das temporäre Abweisen der zu sendenden E-Mail durch den Empfänger wird nicht ausgewertet und ein erneuter Zustellversuch wird nicht unternommen. Sich selbständig über E-Mail verbreitende Viren werden auf diese Weise abgewiesen, da sie ebenfalls keinen erneuten Zustellversuch unternehmen. Es wird empfohlen die Option »Greylist learning only (no mail rejection)« ca. einen Monat zu nutzen, bevor die Option »Use Greylisting« aktiviert wird. Durch die Option »Greylist learning only (no mail rejection)« befindet sich die SEPPmail Appliance bezüglich der Greylisting Funktion in einem Lernmodus und weist keine E-Mails temporär zurück.
	Use Antispam Engine (Note: remember to activate in ruleset)	Dieser Parameter bewirkt, dass der SPAM-Filter auf dem SEPPmail-System aktiviert wird. Die Konfiguration des SPAM-Filters wird im Ruleset Generator im Menü »Mail Processing« 67 durchgeführt.
	Use Antivirus Engine (Note: remember to activate in ruleset)	Dieser Parameter bewirkt, dass der Virenscanner auf dem SEPPmail System aktiviert wird. Die Konfiguration des Virenscanners wird im Ruleset Generator im Menü »Mail Processing« 67 durchgeführt.
	Require HELO command	Dieser Parameter bewirkt, dass geprüft wird, ob der sendende E-Mail-Server das HELO Kommando beim Verbindungsaufbau mit SEPPmail verwendet. Ist dies nicht der Fall, werden bei Aktivierung dieses Parameters keine E-Mails angenommen.
	PTR check (reverse DNS lookup)	SPAM-Versender benutzen häufig E-Mail-Server die nicht im DNS engetragen sind. Wenn diese Option aktiviert wird, werden keine E-Mails von E-Mail-Servern angenommen die keinen Eintrag im DNS haben.
	Check if sender domain is valid	Mit dieser Option aktivieren Sie die Überprüfung des Domain-Teils der Absender E-Mail-Adresse jeder von extern eingehenden E-Mail. Existiert im DNS kein Eintrag für diese Domain, so wird die E-Mail nicht angenommen.

Parameter		Beschreibung
	Require valid hostname in HELO command	Aktivieren Sie diese Option, wenn E-Mails nur von den E-Mail-Servern angenommen werden sollen, die sich mit einem gültigen Hostnamen melden. Existiert im DNS kein Eintrag für diesen Hostnamen, so wird die E-Mail nicht angenommen.
	Require fully qualified hostname in HELO command	Aktivieren Sie diese Option, wenn E-Mails nur von den E-Mail-Servern angenommen werden sollen, die sich mit einem vollständigen Hostnamen (FQDN = Fully qualified domain name) identifizieren.
	Limit incoming connections for SMTP per IP	Mit dieser Einstellung limitieren Sie die Anzahl paralleler Verbindungen je IP. Es soll so verhindert werden, dass einzelne Server SEPPmail überlasten können.
optional Settings		
	Greylist learning only (no mail rejection)	Dieser Parameter aktiviert den Greylisting-Lernmodus. Dabei wird die Datenbank mit den für den Greylisting-Betrieb benötigten Informationen aufgebaut. Nutzen Sie diese Option ca. einen Monat, bevor Sie den aktiven Greylisting-Modus »Use Greylisting« aktivieren und verwenden.
	Strict PTR check (reserse DNS lookup)	Bei Nutzung dieser Option wird für die Annahme von E-Mails vorausgesetzt, dass die IP-Adresse des sendenden E-Mail-Servers in seinen Hostnamen im DNS aufgelöst werden kann (PTR) und dass der Hostname wieder auf die entsprechende IP-Adresse zeigt (A Record).

Sektion »Blacklists«

Parameter	Beschreibung
Add Blacklist (RBL)	E-Mail-Server werden aufgrund von SPAM-Aktivitäten in Blacklists aufgenommen. Diese Listen werden durch verschiedene Anbieter im Internet gepflegt. Um E-Mails abzuweisen die von solchen E-Mail-Servern an Sie gesendet werden, tragen Sie den Namen der entsprechenden Realtime Blackhole Lists (RBL) in diesem Eingabefeld ein.

Sektion »Manual Blacklisting / Whitelisting«

Parameter	Beschreibung
add acccess entry	In diesem Menüpunkt können Sie IP-Netzwerke blockieren oder explizit zulassen aus denen ein E-Mail Server versucht eine E-Mail an das SEPPmail System zu senden. Tragen Sie dazu das IP-Netzwerk, die Aktion und einen Kommentar in die entsprechende Eingabefelder ein. network : <IP-Netzwerk oder IP-Host Adresse>

Parameter	Beschreibung
	action : <Aktion> comment : <Kommentar zum Eintrag> Der Parameter »action« kann folgende Werte annehmen: accept | reject accept : explizit zulassen reject : blockieren **Beispiel:** Um alle E-Mails die aus dem IP-Netzwerk Bereich 186.56.148.x gesendet werden zu verwerfen, geben Sie den IP-Netzwerk Teil 186.56.148 ein und definieren Sie die Aktion »reject«. Netzwerke, aus denen Sie die Annahme von gesendeten E-Mails explizit zulassen möchten, deklarieren Sie hingegen mit der Aktion »accept«.

6.5.2 Zu verwaltende E-Mail-Domains einrichten

Menü »Mail System«

Sektion »Managed Domains«

Zum Erstellen einer neuen E-Mail-Domain wählen Sie in der Konfigurationsoberfläche die Schaltfläche »Add Domain...«.

Parameter	Beschreibung
Domain Name	Tragen Sie im Bereich »Domain Name« den oder die E-Mail-Domainnamen ein, die Sie mit Ihrer Appliance verwalten möchten. Hierbei handelt es sich um Ihre Domain(s), passend zu den E-Mail-Adressen Ihrer Organisation. Wenn Sie beim Anlegen mehrere E-Mail-Domainnamen im Eingabefeld eintragen, separieren Sie diese jeweils mit einem Leerzeichen.
Forwarding Server IP or MX name	Im Bereich »Forwarding Server IP or MX name« tragen Sie die IP-Adresse oder den Hostnamen des für die E-Mail-Domain zuständigen E-Mail-Servers ein. Stellen Sie sicher, dass SEPPmail den entsprechenden E-Mail-Server unter der angegebenen IP-Adresse oder dem Hostnamen falls notwendig erreichen kann. Die Appliance wird eingehende E-Mails der definierten Domain(s) entschlüsseln und an den entsprechenden E-Mail-Server weiterleiten.
Assign to customer	Wählen Sie den Kunden aus, dem diese E-Mail-Domain zugeordnet werden soll.

6.5.3 Ausgehenden E-Mail-Verkehr steuern

Menü »Mail System«

Sektion »Outgoing Server«

Wenn SEPPmail E-Mails direkt an externe E-Mail-Empfänger senden soll, wählen Sie die Option »Use built-in mail transport agent«. Falls der externe Versand durch einen bestehenden E-Mail-Server erfolgen soll, definieren Sie den entsprechenden Server als »Outgoing Server«. Sollte der E-Mail-Server eine Authentifizierung erfordern, geben Sie den Benutzernamen und das Kennwort ein.

6.5.4 TLS-Verschlüsselung pro Domäne einrichten

Menü »Mail System«

Sektion »TLS settings«

Um ausgehende E-Mails via TLS-Transportverschlüsselung zu übermitteln fügen Sie die E-Mail-Domain des Empfängers hinzu. Klicken Sie auf die Schaltfläche »Add TLS Domain...«.

Parameter	Beschreibung
Domain Name	Name der E-Mail-Domain des Empfängers
Optional Forwarding Server Address	IP-Adresse oder Hostname des für die Empfänger E-Mail-Domain zuständigen E-Mail-Servers

Sektion »TLS Settings«

TLS-Einstellung	Beschreibung
None	Keine TLS-Verschlüsselung.
May	E-Mails werden über einen TLS-verschlüsselten Kanal versendet, falls der empfangende E-Mail-Server TLS-Verschlüsselung unterstützt.
Encrypt	E-Mails werden nur versendet, falls der Versand mittels TLS-Verschlüsselung möglich ist.
Verify	E-Mails werden nur versendet, falls der Versand via TLS-Verschlüsselung möglich, und das SSL-Zertifikat des empfangenden E-Mail-Servers gültig ist.
Secure	E-Mails werden nur versendet, falls der Versand via TLS-Verschlüsselung möglich, und das SSL-Zertifikat des empfangenden E-Mail-Servers gültig ist und der Name des E-Mail-Servers gemäß Zertifikat erfolgreich überprüft werden kann. Diese Prüfung kann kann nicht bei der Verwendung von Wildcard-SSL-Zertifikaten eingesetzt werden. Verwenden Sie die TLS-Einstellung »Fingerprint«, falls der E-Mail-Server an den Sie ausgenende E-Mails via TLS versenden wollen ein Wildcard-SSL-Zertifikat verwendet. Erhalten Sie beim Versenden einer E-Mail via TLS-Transportverschlüsselung die Logmeldung »...status=deferred (Server certificate not verified)«, so überprüfen Sie das SSL-Zertifikat des empfangenden E-Mail-Servers auf die Verwendung eines Wildcard-Zertifikats. Weiter unten wird das Vorgehen beschrieben.
Fingerprint	E-Mails werden nur versendet, falls der Versand via TLS-Verschlüsselung möglich ist und das SSL-Zertifikat des empfangenden E-Mail-Servers dem definierten Fingerprint entspricht. Als Fingerprint wird SHA1 unterstützt. Wie Sie den Fingerprint eines SSL-Zertifikats auslesen wird weiter unten beschrieben.

Überprüfen des empfangenden E-Mail-Servers auf die Verwendung eines Wildcard-SSL-Zertifikats

Ob ein E-Mail-Server ein Wildcard-SSL-Zertifikat verwendet kann sehr einfach mit dem Kommandozeilentool »OpenSSL« durchgeführt werden.

Beispiel:

```
# openssl s_client -starttls smtp -crlf -connect xxx.xxx.xxx.xxx:25
```

Ersetzen Sie die IP-Adresse xxx.xxx.xxx.xxx durch die tatsächliche IP-Adresse des Zielservers oder verwenden Sie den Hostnamen.

```
# openssl s_client -starttls smtp -crlf -connect postini.com.s8a1.psmtp.com:25
```

Hier sehen Sie das Ergebnis der Abfrage. Anhand des Zertifikats-Subject im Parameter »CN« können Sie feststellen, ob es sich um ein Wildcard-SSL-Zertifikat handelt. In der Antwort wurde der Wert »CN=*.psmtp.com« zurückgegeben. In diesem Fall handelt es sich um ein Wildcard-Zertifikat, welches für alle Hosts der Domain »psmtp.com« verwendet werden kann. Ebenfalls interessant ist der »Parameter X509v3 Subject Alternative Name:«. Als Wert wird hier »DNS:*.psmtp.com« zurückgegeben. In diesem Feld können noch weitere Domains enthalten sein.

```
# openssl s_client -starttls smtp -crlf -connect postini.com.s8a1.psmtp.com:25 |
openssl x509 -text -noout

  depth=1 C = US, O = Google Inc, CN = Google Internet Authority
  .
  .
  Certificate:
         .
         .
        Subject: C=US, ST=California, L=Mountain View, O=Google Inc, CN=*.psmtp.
com
         .
         .
         .
                    X509v3 Subject Alternative Name:
                DNS:*.psmtp.com
```

Die Darstellung der Ausgabe wurde auf die wesentlichen Informationen reduziert.

Auslesen des SHA1-Fingerprint aus dem SSL-Zertifikat des empfangenden E-Mail-Servers

Einen Schritt zuvor wurde beschrieben, wie Sie das vom empfangenden E-Mail-Server verwendete SSL-Zertifikat auslesen können. Dabei ist es nicht relevant, ob es sich hierbei um ein Wildcard-Zertifikat handelt oder nicht.

Den Fingerprint eines SSL-Zertifikats können Sie sehr einfach mir dem Kommandozeilentool »OpenSSL« auslesen.

Beispiel:

```
# openssl s_client -starttls smtp -crlf -connect xxx.xxx.xxx.xxx:25 | openssl x509
-noout -fingerprint
```

Ersetzen Sie die IP-Adresse xxx.xxx.xxx.xxx durch die tatsächliche IP-Adresse des Zielservers oder verwenden Sie den Hostnamen.

```
# openssl s_client -starttls smtp -crlf -connect postini.com.s8a1.psmtp.com:25 |
openssl x509 -noout -fingerprint
```

Als Ergebnis erhalten Sie die folgende Ausgabe:

```
# openssl s_client -starttls smtp -crlf -connect postini.com.s8a1.psmtp.com:25 |
openssl x509 -noout -fingerprint

depth=1 C = US, O = Google Inc, CN = Google Internet Authority
verify error:num=20:unable to get local issuer certificate
verify return:0
250 HELP
SHA1 Fingerprint=DD:9A:EC:66:E2:43:81:B9:20:2B:75:DB:30:C8:67:CC:9B:B0:D1:99
read:errno=0
```

In der Ausgabe wird der benötigte SHA1 Fingerprint angezeigt. Sie können diesen Wert nun in der Konfiguration verwenden bzw. mit Copy & Paste übernehmen.

6.5.5 SMTP-Einstellungen

Menü »Mail System«

Sektion »SMTP settings«

Parameter	Beschreibung
max. message size (kb)	Maximale Grösse einer E-Mail-Nachricht
Postmaster address	E-Mail-Adresse des Postmasters
SMTP server HELO string	Festlegen, welchen Namen SEPPmail beim Versand von E-Mails im HELO/EHLO-Befehl verwenden soll.
SMTP bind address (use with care!)	Festlegung der IP-Adresse eines Netzwerk-Interfaces, über welche alle Mails empfangen werden (normalerweise nicht notwendig)
OpenPGP key creation options, automatically send new public keys to users	Falls diese Option aktiviert wird, werden die durch OpenPGP generierten öffentlichen Schlüssel automatisch an die Benutzer versendet

6.5.6 Mail Relaying

Menü »Mail System«

Sektion »Relaying«

Parameter	Beschreibung
Relaying allowed	Netzwerke oder IP-Adressen die SEPPmail als E-Mail-Relay für ausgehende E-Mails verwenden können. Stellen Sie sicher, dass nur interne Netzwerke bzw. IP-Adressen, die unter Ihrer Verwaltung stehen, aufgelistet sind. Damit verhindern Sie den mißbräuchlichen Versand von E-Mails über SEPPmail. Die Definition der Netzwerke wird nach der Classless Inter-Domain Routing (CIDR) Notation festgelegt. Diese entspricht zum Beispiel folgenden Werten: • Die Netzmaske 255.255.255.255 entspricht "/32" (einzelne IP-Adresse) • Die Netzmaske 255.255.255.0 entspricht "/24" (Klasse C Netzwerk) • Die Netzmaske 255.255.0.0 entspricht "/16" (Klasse B Netzwerk) • Die Netzmaske 255.0.0.0 entspricht "/8" (Klasse A Netzwerk)
Add Relaying for	Erfassen Sie eine zusätzliche IP-Adresse die eine Releayberechtigung haben soll.

6.5.7 Antispam-Einstellungen

Menü »Mail System«

Sektion »Antispam« -> Bereich »Recommended Settings«

Parameter	Beschreibung
Use Greylisting	Greylisting ist eine Methode zur Spam-Bekämpfung. Dabei werden E-Mails von unbekannten Absendern nicht unmittelbar entgegengenommen, sondern zunächst abgewiesen. Bei legitimen Mails hält der sendende Mailserver die Mails pendent und übermittelt diese zu einem späteren Zeitpunkt nochmals. Beim erneuten Zustellversuch werden die Mails dann angenommen. Es wird bei diesem Mechanismus davon ausgegangen, dass Mailserver und Clients sich an den RFC-Standard für SMTP halten. Spammer benutzen oft keine RFC-konforme Software zum Versenden von Spam-Mails. Sie kommen mit dem Fehler nicht zurecht und merken sich nicht, dass sie es später nochmals versuchen müssten. Sich selbständig verbreitende Viren werden auf diese Weise abgewiesen, da sie ebenfalls keinen zweiten Versuch des Versendens vornehmen. Es wird empfohlen den Parameter »Greylist learning only (no mail rejection)« ca. einen Monat zu nutzen, bevor der

Parameter	Beschreibung
	Parameter »Use Greylisting« aktiviert wird. Durch den Parameter »Greylist learning only (no mail rejection)« befindet sich SEPPmail bezüglich Greylisting in einem Lernmodus und weist keine E-Mails permanent ab.
Use Antispam Engine (Note: remember to activate in ruleset)	Aktivieren Sie diesen Parameter, um das Protection Pack (Anti-spam / Anti-virus) für Anti-SPAM zu nutzen.
Use Antivirus Engine (Note: remember to activate in ruleset)	Aktivieren Sie diesen Parameter, um das Protection Pack (Anti-spam / Anti-virus) für Anti-Virus zu nutzen.
Require HELO command	Es wird geprüft, ob der sendende Mailserver das HELO Kommando benutzt. Ist dies nicht der Fall, werden bei Aktivierung dieser Option keine Mails angenommen.
PTR check (reverse DNS lookup)	Spammer benutzen oft nicht in DNS eingetragene Mailserver. Wenn diese Option aktiv ist, werden keine Mails von entsprechenden Mailservern angenommen.
Check if sender domain is valid	Es werden bei Nutzung dieser Option nur Mails angenommen, wenn der vom Mailserver angegebene Mail Exchanger Host auf die entsprechende IP-Adresse zeigt.
Require valid hostname in HELO command	Ist diese Option aktiv, werden Mails nur angenommen, wenn sich der Mailserver mit einem gültigen Hostnamen meldet.
Require fully qualified domain name in HELO command	Aktivieren Sie diese Option, wenn nur Mails von Mailservern angenommen werden sollen, welche sich mit einem vollständigen Hostnamen (FQDN = Fully qualified domain name) identifizieren.
Limit incoming connections for SMTP per IP	Mit dieser Einstellung limitieren Sie die Anzahl paralleler Verbindungen je IP. Es soll so verhindert werden, dass einzelne Server SEPPmail überlasten können.

Sektion »Antispam« -> Bereich »Optional Settings«

Parameter	Beschreibung
Greylist learning only (no mail rejection)	Diese Option aktiviert den Greylisting-Lernmodus. Dabei wird die Datenbank mit den für den Greylisting-Betrieb benötigten Informationen aufgebaut. Nutzen Sie diese Option ca. einen Monat, bevor Sie den aktiven Greylisting-Modus Use Greylisting verwenden.
Strict PTR check (reverse DNS lookup)	Bei Nutzung dieser Option wird für die Annahme von Mails vorausgesetzt, dass die Hostadresse des sendenden Mailservers im DNS über seine IP-Adresse aufgelöst werden kann (PTR) und dass der Namenseintrag auch wieder auf die entsprechende IP-Adresse zeigt (A Record).

6.5.8 Blacklists / Whitelists verwalten

Menü »Mail System«

Sektion »Blacklists / Whitelists«

E-Mail-Server werden aufgrund von Spamming-Aktivitäten in Blacklists aufgenommen. Diese Listen werden durch verschiedene Anbieter im Internet gepflegt. Um E-Mails von solchen E-Mail-Servern abzuweisen, tragen Sie entsprechende Realtime Blackhole Lists (RBL) in der Rubrik »Blacklists« ein.

Wenn Sie manuell Netzwerke blockieren oder explizit zulassen möchten, tragen Sie diese in der Rubrik »Manual Blacklisting / Whitelisting« ein.

Um beispielsweise alle E-Mails vom Netzwerk 186.56.148.x zu verwerfen, geben Sie 186.56.148 ein und definieren Sie die Aktion »reject«. Netzwerke, von denen Sie die Annahme von Mails explizit zulassen möchten, deklarieren Sie hingegen mit der Aktion »accept«.

6.6 Menüpunkt "Mail Processing"

Dieses Kapitel beschreibt die Verwaltung des E-Mail-Regelwerks.

Folgende Vorgänge werden in den kommenden Abschnitten beschrieben:

6.6.1 GINA Webmail-Schnittstelle

GINA ist die neue Standard-Schnittstelle für Secure-Webmail. Mit der Version 6 setzt SEPPmail einen neuen Secure-E-Mail-Standard. Die Übertragung digital signierter und verschlüsselter E-Mails wird einfacher denn je – für Absender und Empfänger gleichermaßen.

Die Secure-E-Mail-Plattform SEPPmail V6 GINA darf als weltweit einfachste, vielseitigste und trotzdem komfortabelste Lösung für die hoch sichere E-Mail-Übertragung bezeichnet werden. Sie besticht durch zahlreiche Highlights.

Modernes User-Interface
- intuitiv bedienbare Benutzerschnittstelle
- Maximaler Komfort beim Empfangen und Öffnen gesicherter E-Mails via Webmail
- Benutzerfreundliche Einbindung mobiler Endgeräte

Portalfunktionen
- Externe Benutzer erhalten die Möglichkeit, jederzeit verschlüsselte E-Mails an interne Mitarbeiter zu senden
- Externe Benutzer können sich selbständig via Portal registrieren
- Bereits bestehende Keys (S/MIME oder PGP) lassen sich durch die externen User selbständig hochladen

Customizing - Anpassung des Layouts an eigene Bedürfnisse
- Adaption sämtlicher GINA-Komponenten an individuelle Bedürfnisse – ermöglicht beispielsweise die Umsetzung von Corporate-Design-Vorgaben
- Integration in Firmen-Websites, Portale etc.
- Einbindung beliebiger Sprachen (ideal für international tätige Unternehmen sowie für Cloud-Anbieter)

Self Service Passwort Management (SSPM)
- Vergessene Passwörter können vom Empfänger automatisch und ohne Sicherheitsrisiken via Mobile Phone neu generiert bzw. angefordert werden

Interne Verschlüsselung (IME)
- Komfortable, firmeninterne Verschlüsselung vertraulicher E-Mails – vom Arbeitsplatz des Absenders bis zum Desktop des Empfängers; dadurch sind vertrauliche E-Mails im gesamten Firmennetz vor unerlaubtem Zugriff geschützt

6.6.1.1 GINA Domains erstellen

Menü »Mail Processing«

Um eine neue GINA-Domain zu erstellen, klicken Sie in der Rubrik »GINA domains« auf die Schaltfläche »Create new GINA domain...«.

Sektion »Create new GINA Domain«

Parameter	Beschreibung
Description	eine Beschreibung der neuen GINA-Domain
Hostname	Name des Hosts der neuen GINA-Domain. Dieser Name ist Bestandteil der URL, unter der Webmails abgerufen werden, z. B. https://secmail.cusomer.com/customer

Bestätigen Sie die Erstellung einer neuen GINA-Domain mit einem Klick auf die Schaltfläche »Create«.

6.6.1.2 GINA Domains löschen

Menü »Mail Processing«

Um eine bestehende GINA-Domain zu löschen, wählen Sie die GINA-Domain im Menü »Mail Processing« -> »GINA domains« aus und klicken Sie die Schaltfläche »Delete«.

Bestätigen Sie das Löschen einer bestehenden GINA-Domain mit einem Klick auf die Schaltfläche » Delete«.

6.6.1.3 GINA Domains verwalten

Menü »Mail Processing«

Sie können GINA-Einstellungen bearbeiten, indem Sie die entsprechende GINA-Domain in der Rubrik » GINA domains« auswählen und auf die Schaltfläche Edit... klicken. Die Standard GINA-Domain hat den Namen [default].

Sie können Parameter in den folgenden Kategorien verwalten:

- Hostname 69
- Secure Webmail Port 69
- Secure Webmail Key and certificate 69
- Master Template 69
- Admin 69
- Extended settings 69
- Terms of use 72
- Language settings 72
- Security 72
- Certificate login 74

Diese Sektionen werden nachfolgend einzeln erläutert.

Sektion »Secure GINA Host«

In der Sektion »Secure GINA Host« können Sie für Werte für Hostname, Port, Key and certificate der GINA-Domain hinterlegen. Dieser Hostname ist Bestandteil der URL, unter der GINA-Nachrichten abgerufen werden, z.B. https://secmail.customer.com. Falls Sie die Funktion »Virtual Hosting« aktiviert haben, können Sie für die jeweilige GINA-Domain einen eigenen Port vergeben und ein eigenes SSL-Zertifikat hinterlegen.

Sektion »Master Template«

Diese Sektion wird bei Auswahl der GINA-Domain [default] nicht angezeigt.

In der Sektion »Master Template« wählen Sie die GINA-Domain aus, die Sie als Vorlage verwenden möchten. Die Einstellungen werden von dieser GINA-Domain übernommen. Dies erleichtert Ihnen die Verwaltung von Optionen, welche für mehrere GINA-Domains Gültigkeit haben sollen.

Bei Auswahl der Standard GINA-Domain [default], wird diese als Vorlage zur Übernahme von Einstellungen verwendet. In welchem Umfang Einstellungen übernommen werden, legen Sie in den einzelnen Sektionen fest, die nachfolgend detailliert erläutert werden.

Sektion »Admin«

In der Sektion »Admin« können Sie eine E-Mai-Adresse für den Administrator erfassen, welcher eine Benachrichtigung als E-Mail erhält, wenn einen GINA-Empfänger sein Kennwort zurücksetzen lassen möchte. Hierzu muss das Security Level auf »Reset by hotline« eingestellt sein.

Sektion »Extended settings«

Parameter	Beschreibung
Use settings from master template	Aktivieren Sie dieses Kontrollkästchen, falls Sie die Einstellungen vom Master Template übernehmen möchten.
Default Forward Page	URL die verwendet wird, falls die GINA-Oberfläche direkt, statt über eine GINA-Nachricht, aufgerufen wird (optional).
Always zip HTML attachments when encrypting mail with GINA technology	Verwenden Sie diese Einstellung, wenn der verschüsselte E-Mail-Teil einer GINA-Nachricht im ZIP- anstatt im HTML-Format angehängt werden soll. Diese Einstellung wird benötigt, wenn

Parameter	Beschreibung
(for OWA compatibility, for single mails use [owa] in subject)	der Empfänger Outlook Web Access (OWA) verwendet, da GINA-Nachrichten im HTML-Format aus OWA nicht entschlüsselt werden können. Um die Einstellung nur bei einzelnen E-Mails zu nutzen, kann der Begriff [owa] als Steuerkommando in der Betreffzeile verwendet werden. Sollte eine GINA-Nachricht im HTML-Format an einen OWA-Empfänger gelangen, erkennt die SEPPmail-Appliance dies. Der Absender wird aufgefordert, die E-Mail nochmal zu schicken. Gleichzeitig wird im GINA-Benutzerkonto des Empfänger der Parameter »Zip Attachement« aktiviert. Der Empfänger kann eine mit dieser Einstellung erzeugte GINA-Nachricht problemlos lesen.
"Send copy to myself" checked by default when writing GINA mails	Diese Einstellung bewirkt, dass bei GINA-Benutzern die Option »send copy to myself« (Kopie ausgehender E-Mails an sich selbst schicken) standardmässig aktiviert ist.
Sender always receives notification when recipient reads mail in web viewer (overrides user setting)	Aktivieren Sie diese Einstellung, um eine Benachrichtigung zu erhalten, wenn ein ein Empfänger eine GINA-Nachricht im GINA-Portal öffnet und liest. Die benutzerspezifischen Einstellungen werden überschrieben.
Allow account self-registration in GINA portal without initial mail	Ermöglicht die Registrierung eines neuen GINA-Empfängers ohne das dieser zuvor eine GINA-Nachricht erhalten hat. Der Benutzer kann sich selbst über das GINA-Portal als GINA-Empfänger registrieren. Er erhält eine Anmeldebestätigung via E-Mail mit einem Aktivierungs-Link. Nach bestätigen des Aktivierungs-Link kann das neue GINA-Benutzerkonto genutzt werden. Weitere Informationen erhalten Sie im Kapitel GINA Selbstregistrierung über Webmail Portal 80.
Enable S/MIME certificate / PGP key search and management in GINA	Ermöglicht einem GINA-Benutzer zusätzlich einen vorhandenen PGP oder S/MIME Public-Key im Zertifikatsspeicher der SEPPmail-Appliance abzulegen. Der GINA-Benutzer kann dann auch via PGP oder S/MIME verschlüsselte E-Mails erhalten. Weitere Informationen erhalten Sie im Kapitel GINA S/MIME und PGP Schlüsselsuche über Webmail Portal 83. Sie müssen diese Option aktivieren, um die folgende Option »Allow unregistered users to search public keys/certificates of internal users« aktivieren zu können. Sonst ist die folgende Option nicht aktivierbar.
Allow download of public domain keys/domain certificates (Note: You must assign "Use GINA Settings" under Mail System Settings / Managed Domains)	Ermöglicht es externen nicht registrierten Benutzern selbstständig über das GINA-Portal nach vorhandenen PGP oder S/MIME Domain-Keys der angelegten Managed-Domains zu suchen und diese herunterzuladen.
Allow unregistered users to search public keys/	Ermöglicht es externen nicht registrierten Benutzern selbstständig über das GINA-Portal nach vorhandenen PGP

Parameter	Beschreibung
certificates of internal users (and domain keys, if enabled above)	oder S/MIME Public-Keys interner Benutzer zu suchen und diese herunterzuladen.
Allow GINA users to write new mails (not reply)	Aktivieren Sie diese Einstellung, wenn die Schaltfläche zum Erzeugen neuer E-Mails im GINA-Portal aktiv sein soll. Ein GINA-Benutzer kann dann an interne Mitarbeiter E-Mails aus dem GINA-Portal senden. Sie können über diese Funktion Nachrichten ausschließlich an E-Mail-Adressen interner Mitarbeiter senden. Der E-Mail Versand an externen E-Mail-Adressen ist nicht möglich.
Do not allow GINA users to edit recipient when replying to e-mails	Aktivieren Sie diesen Parameter wenn Sie verhindern möchten, dass beim Beantworten einer GINA-Nachricht die E-Mail-Adresse des Empfängers verändert werden kann.
Allow messages to be downloaded as Outlook message (.msg) files	Aktivieren Sie diese Einstellung, wenn die Schaltfläche Outlook im GINA-Frontend angezeigt werden soll. Sie können dann die entschlüsselte E-Mails im Outlook-Format ".msg" im lokalen Dateisystem speichern und nachträglich in Outlook importieren. Die Nachricht wird im Klartext abgelegt.
Allow messages to be downloaded as MIME (.eml) files	Aktivieren Sie diese Einstellung, wenn die Schaltfläche Nachricht speichern im GINA-Frontend angezeigt werden soll. Sie können dann die entschlüsselte E-Mails im Standard-Format ".eml" im lokalen Dateisystem speichern und nachträglich in einem E-Mail Client importieren. Die Nachricht wird im Klartext abgelegt.
When encrypting mail with GINA technology, use text-only emails (no HTML emails)	Die Kurzinformation für den GINA-Empfänger wird als nur Text Nachricht ausgeführt und nicht als HTML Nachricht.

Sektion »Large File Management«

Parameter	Beschreibung
Enable Large File Management	Aktiviert oder Deaktiviert die Funktion »Large File Management«.
Days to store Large Files	Zeitspanne in Tagen zur Vorhaltung der zwischengespeicherten Dateien.
Threshold for Large Files	Größe der E-Mail in KB ab der eine E-Mail via »LFM« verarbeitet wird.
Limit Large Files per Day	Anzahl der Dateien die ein Benutzer pro Tag via »LFM« versenden kann.

Für den Betrieb von Large File Management ist es erforderlich, einen zusätzlichen Bereich auf dem lokalen Datenspeicher einzurichten. Dieser Bereich wird im Menü »Home« als »LFM store« angezeigt.

Zum Einrichten des zusätzlichen Datenspeichers für Large File Management kontaktieren Sie Ihren Support.

Sektion »Terms of use«

Parameter	Beschreibung
Use settings from master template	Aktivieren Sie dieses Kontrollkästchen, falls Sie die Einstellungen vom Master Template übernehmen möchten.
Require new users to accept terms of use	Aktivieren Sie dieses Kontrollkästchen, wenn jeder neue GINA-Benutzer beim erstmaligen Aktivieren des GINA-Benutzerkontos spezielle Nutzungsbedingungen akzeptieren muß. Die detailierten Nutzungsbedingungen können unter der eingetragenen URL eingesehen werden.
Terms of use URL (required)	Geben Sie hier die URL ein unter der die Nutzungsbedingungen im Internet eingesehen werden können. (z.B. http://www.customer.com/termsofuse.html)

Sektion »Language settings«

Parameter	Beschreibung
Default language	Festlegen der Standard-Sprache für das GINA-Portal
Available Languages	Aktivieren, Deaktivieren und Hinzufügen bestehender und/oder neuer Sprachen Erfahren Sie mehr dazu im Kapitel GINA Webmail-Sprachunterstützung verwalten 77.

Wenn Sie die Einstellungen vom Master Template übernehmen möchten, klicken Sie auf das Kontrollkästchen »Use settings from master template«. Diese Option ist nur dann sichtbar, wenn Sie sich in der Konfuration einer zusätzlich angelegten GINA-Domain befinden.

Sektion »Security«

Parameter	Beschreibung
Choose how the user can retrieve lost passwords	Definiert das Standard-Verfahren für einen Kennwort-Reset innerhalb der GINA-Domain
Minimum password length	Definiert die minimale Länge eines Kennworts
Password Complexity	Definiert die Komplexität des Kennworts

Parameter »Choose how the user can retrieve lost passwords«

Wählen Sie das Verfahren für den Kennwort-Reset, damit ein externer GINA-Benutzer sein GINA-Benutzerkennwort zurücksetzen kann. Danach wird je nach ausgewählem Verfahren für den Kennwort-Reset eines der folgenden Verfahren verwendet:

Auswahlwert »default (Reset by hotline)«

Der Wert »default« bezieht sich auf die für die jeweilige GINA-Domain ausgewählte globale Standardeinstellung. Dieses wird innerhalb der Konfiguration der GINA-Domain in der Sektion »Security« eingestellt.

Auswahlwert »Reset by Email verification«

Der externe GINA-Benutzer kann sein Kennwort selbstständig zurücksetzen. Zur Aktivierung und Bestätigung dieser Aktion erhält er eine E-Mail-Benachrichtigung mit einem Aktivierungslink. Nach dem Bestätigen dieses Aktivierungslinks wird das vom externen Benutzer zuvor neu eingegebene Kennwort aktiviert. Ein Login mit dem neu gesetzten Kennwort ist nun möglich.

Auswahlwert »Reset by hotline«

Der externe GINA-Benutzer kann sein Kennwort nicht selbstständig zurücksetzen. Er gibt dazu seine Rufnummer an, unter der er für den Support erreichbar ist. Nach Überprüfung durch die Sicherheitsfrage erhält er vom Support-Mitarbeiter ein neues Einmalkennwort zum nächsten Login. Nach dem Login ist es erforderlich, ein neues persönliches Kennwort erfassen. Ein Login mit dem neu gesetzten Kennwort ist nun möglich.

Auswahlwert »Reset by hotline, no reminder question/answer«

Der externe GINA-Benutzer kann sein Kennwort nicht selbstständig zurücksetzen. Er gibt dazu seine Rufnummer an, unter der er für den Support erreichbar ist. Eine Überprüfung durch die Beantwortung einer Sicherheitsfrage ist nicht erforderlich. Beim Erstmaligen Initialisieren des GINA-Benutzerkontos ist es nicht erforderlich, dass der Benutzer eine Sicherheitsfrage angibt. Der Benutzer erhält vom Support-Mitarbeiter ein neues Einmalkennwort zum nächsten Login. Nach dem Login ist es erforderlich, ein neues persönliches Kennwort erfassen. Ein Login mit dem neu gesetzten Kennwort ist nun möglich.

Diese folgenden Möglichkeiten für das Zurücksetzen eines Kennworts können nur im Rahmen der Funktion Self Service Passwort Management (SSPM) ausgeführt werden. Siehe GINA Self Service Passwort Management 82

Auswahlwert »Reset by SMS«

Der externe GINA-Benutzer kann ein neues Kennwort via SMS auf sein Mobiltelefon anfordern. Dieses neue Einmalkennwort verwendet der Benutzer für den nächsten Login. Dabei muss er ein neues persönliches Kennwort erfassen. Ein Login mit dem neu gesetzten Kennwort ist nun möglich.

Beim Reset des Kennworts via SMS muss die Mobilfunkrufnummer im Benutzerprofil des Benutzers hinterlegt worden sein.

Beinhaltet ein ausgewähltes Verfahren zur Kennwortrücksetzung die Option SMS, so ist es ebenfalls erforderlich den SMS-Versand im Menü »Mail Processing« einzurichten.

Auswahlwert »Let user choose between hotline and SMS«

Der externen GINA-Benutzer kann zum anfordern eines neuen Kennworts zwischen den beiden Optionen »Hotline« und »SMS« auswählen.

Parameter »Mobile Number«

Beinhaltet die Mobilfunkrufnummer des GINA-Benutzers, fals diese vom Benutzer beim Verwalten seines Benutzerkontos hinterlegt wurde. Für den Support besteht die Möglichkeit dem Benutzer bei Bedarf ein neues One-Time Kennwort (Einmalkennwort) als SMS zu senden. Klicken Sie dazu auf die Schaltfläche »SMS password reset«. Es wird ein neues One-Time Kennwort automatisch durch SEPPmail generiert und via SMS gesendet.

Parameter »Minimum password length« und »Password Complexity«

Parameter	Beschreibung
Minimum password length	Minimale Passwortlänge (Standard: 8 Zeichen)
Must Contain at least one lower case letter	Das Passwort muss mindestens einen Kleinbuchstaben beinhalten.
Must Contain at least one upper case letter	Das Passwort muss mindestens einen Grossbuchstaben beinhalten.
Must Contain at least one number	Das Passwort muss mindestens eine numerisches Zeichen enthalten.
Must Contain at least one special character	Das Passwort muss mindestens ein Sonderzeichen enthalten.
Must not contain own name or mail address	Das Passwort darf den eigenen Namen oder die eigene E-Mail-Adresse nicht beinhalten.
Must be different from previous password	Das Passwort darf nicht das Gleiche sein, wie das Vorherige.

Wenn Sie die Einstellungen vom Master Template übernehmen möchten, klicken Sie auf das Kontrollkästchen »Use settings from master template«.

Sektion »Certificate login«

In der Sektion »Certificate Login« können Sie Root-CA-Zertifikate hinterlegen (z.B. SuisseID) die für eine GINA-Benutzer Identifikation verwendet werden können. Jeder GINA-Benutzer muss in seinem Webbrowser ein Zertifikat installiert haben, welches vor einer der hier hinterlegten Root-CAs ausgestellt wurde.

Wenn Sie die Einstellungen vom Master Template übernehmen möchten, klicken Sie auf das Kontrollkästchen »Use settings from master template«.

6.6.1.4 GINA Layout verwalten

Menü »Mail Processing«

Zum Anpassen des Layouts einer bestehenden Webmail-Domain wählen Sie innerhalb des Konfigurationsmenüs der GINA-Domain die Schaltfläche »Edit GINA Layout«. Sie befinden sich nun in der Konfiguration für das GINA-Layout der jeweiligen GINA-Domain.

Sie können Parameter in den folgenden Kategorien verwalten:

Sektion »Header Logo«

In dieser Sektion können Sie eine zusätzliche Grafik im Bereich »Header Logo« der Webmail-Oberfläche einbinden. Die Anzeige dieser Grafik aktivieren Sie in der Sektion Extended Settings 76.

Sektion »Company Logo«

Um die GINA-Oberfläche an Corporate-Design Vorgaben anzupassen haben Sie die Möglichkeit in dieser Sektion ein Firmenlogo einzufügen. Weitere Anpassungen können Sie in der Standard CSS-Datei der GINA-Oberfläche vornehmen. Siehe GINA Webmail-Layout verwalten 76

Sektion »Favourites Icon«

In dieser Sektion können Sie ein optionales Favicon im Dateiformat .ico einfügen. Dieses Favicon wird dann als Grafik an Anfang der Adresszeile im Webbrowser angezeigt.

Sektion »Footer Logo«

In dieser Sektion können Sie eine zusätzliche Grafik im Bereich »Footer Logo« der GINA-Oberfläche einbinden. Die Anzeige dieser Grafik aktivieren Sie in der Sektion Extended Settings 76.

Sektion »Background Image«

In dieser Sektion können Sie eine Grafik als Hintergrund für die GINA-Oberfläche einzufügen. Weitere Eigenschaften können Sie in der Sektion GINA Webmail-Layout verwalten 76 verwalten.

Sektion »GINA CSS«

In dieser Sektion verwalten Sie alle GINA CSS Eigenschaften. Eine CSS-Datei wird verwendet, um das Layout der GINA-Oberfläche anzupassen. Dabei sind die Daten und die Formatierung getrennt voneinander. Wenn Sie sich mit CSS beschäftigen können Sie die GINA-Oberfläche z.B. an Ihre Corporate-Vorgaben anpassen und so einfach in Ihre Webseite integrieren.

Sektion »Extended settings«

In dieser Sektion können Sie die zuvor eingerichteten Optionen zum Anzeigen in der GINA-Oberfläche aktivieren oder deaktivieren.

Parameter	Beschreibung
Disable "Powered by ..." Logo in Webmail-viewer	Bei Aktivierung dieser Option wird der Text "Powered by SEPPmail" beim Aufruf einer GINA-Nachricht nicht angezeigt.
Enable Header logo on Login page	aktivieren Sie das Header Logo innerhalb der GINA-Anmeldung
Enable Header logo an all other pages	aktivieren Sie das Header Logo innerhalb der gesamten GINA-Oberfläche
Enable Footer logo on Login page	aktivieren Sie das Footer Logo innerhalb der GINA-Anmeldung
Enable Footer logo an all other pages	aktivieren Sie das Footer Logo innerhalb der gesamten GINA-Oberfläche
Enable Footer text an Login page	aktivieren Sie den Footer Text innerhalb der GINA-Anmeldung
Enable Footer text an all other pages	aktivieren Sie den Footer Text innerhalb der gesamten GINA-Oberfläche

Die Einstellungen für den Footer Test finden Sie in der Sektion GINA Webmail-Sprachunterstützung verwalten 78.

6.6.1.5 GINA Sprachunterstützung verwalten

In der Sektion »Language Settings« haben Sie die Möglichkeit, die bereits im Lieferumfang enthaltenen Übersetzungen anzupassen oder eigene Übersetzungen für zusätzliche Sprachunterstützungen der GINA-Schnittstelle hinzuzufügen.

Sie können in dieser Sektion die folgenden Einstellungen vornehmen:

Edit translations... 77
Download 79
Add new... 79

Parameter/Schaltfläche	Beschreibung
Default language	Einstellen der Standard-Sprache für die GINA-Schnittstelle
Available Languages	Herunterladen und Anpassen einer vorhandenen Sprachvariante für die GINA-Schnittstelle
Schaltfläche Edit Translations	Anpassen der Übersetzung einer vorhandenen Sprachvariante
Schaltfläche Download	aktuelle Übersetzung der jeweiligen Sprache herunterladen und ggf. als Vorlage für eigene Übersetzungen verwenden
Schaltfläche Change	speichern der durchgeführten Änderungen in dieser Sektion
Schaltfläche Add new	hinzufügen Übersetzung für eine neuen Sprachvariante

Die folgenden Übersetzungen sind im Auslieferungszustand enthalten:

- Englisch - English(e)
- Spanisch - Spanish(s)
- Deutsch - German (d)
- Französisch - French (f)
- Italienisch - Italian (i)

Wenn Sie die Einstellungen vom Master Template übernehmen möchten, klicken Sie auf das Kontrollkästchen »Use settings from master template«. Diese Option ist nicht für die Einstellungen der Standard Webmail Domain »[default]« sichtbar sondern wird nur in zusätzlich angelegten Webmail Domains angezeigt.

Schaltfläche »Edit translations...«

Sie können über die Schaltfläche »Edit translations...« die aktuelle Übersetzung bestimmter Textbestandteile der GINA Schnittstelle selbst und Textbestandteile der Kurzinformationstext der GINA-Nachricht anpassen.

Innerhalb dieser Sektion können Sie mit den folgenden Schaltflächen navigieren:

Back	: Rückkehr in die übergeordnete Konfigurationsseite
Advanced View	: Erweitert die Anzeige und ermöglicht die Bearbeitung weiterer Ressourceneinträge der Übersetzung

Normal View	: ist nur Verfügbar wenn zuvor die Schaltfläche »Advanced View« betätigt wurde

Die folgenden Textbestandteile können bearbeitet werden:

Customization 78
Text in Secure Webmail 78
Open hint in Secure Webmail 78
Greeting on Login page 78
Footer text 78
Webmail Password Notification Mail 79

In der Erweiterten Ansicht:

Edit Translation file 79

Sektion »Customization«

Wichtige Anmerkung

- Verwenden Sie keines der reservierten Schlüsselwörter »msgid« und »msgstr« in irgendeinem Textbestandteil.
- Text darf keine Leerzeilen enthalten um einen Zeilenumbruch zu erzeugen. Verwenden Sie
 zum Erzeugen eines Zeilenumbruchs. Jedes
 wird durch einen Zeilenumbruch ersetzt. (z.B. wie in reinen Text E-Mails).
- HTML TAG's sind nicht erlaubt. Sie dürfen nur innerhalb von Textbestandteilen verwendet werden die im Webmail Viewer angezeigt werden.

Sektion »Text in GINA«

Dieser Text wird innerhalb der GINA-Nachricht als Kurzinformationstext angezeigt und enthält Hinweise zur Handhabung dieser E-Mail für den Empfänger.

Sektion »Open hint in GINA«

Dieser Text wird im Anmeldedialog angezeigt, wenn Sie eine Webmail öffnen und sich zur Entschlüsselung anmelden.

Sektion »Greeting on Login page«

Begrüßungstext, nachdem Sie eine GINA-Nachricht zum Entschlüsseln geöffnet haben.

Sektion »Footer text«

Dieser Text wird im Footer-Bereich der GINA-Oberfläche angezeigt und kann ein- und ausgeblendet werden. Siehe GINA Webmail-Layout verwalten 76.

Sektion »GINA Password Notification Mail«

Dieser Text wird in die Passwortbenachrichtigung eingefügt die ein Absender erhält, nachdem er das Erste Mal eine GINA-Nachricht an einen Empfänger versendet hat.

Sektion »Edit Translation file«

Wählen Sie die Schaltfläche »Advanded View«, um den Editor zur Übersetzung der ausgewählten Sprachversion zu erhalten.

In dieser Sektion können Sie die Übersetzung der ausgewählten Sprachversion bearbeiten. Um diesen Bereich auszublenden wählen Sie die Schaltfläche »Normal View«.

Sektion »Download«

Sie können über die Schaltfläche »Download« die aktuelle Übersetzung einer bestehenden Sprachvariante herunterladen und als Basis für eine neue Übersetzung einer zusätzlichen Sprachvariante verwenden.

Sektion »Add new...«

Zum Hinzufügen der Übersetzung für eine neue Sprachunterstützung wählen Sie die Schaltfläche »Add new...«. Sie können die folgenden Parameter erfassen:

Parameter	Beschreibung
Name	Name der neuen Sprache in der jeweiligen Landessprache, z.B. Polski für Polnisch
Please enter the name of the new language in every other of the available languages	Hinzufügen der Übersetzung der vorhandenen Sprachen in der neue Sprachvariante, z.B. Deutsch, German, Allemand, Tedesco, Alemán etc. für Deutsch. Dies sind Pflichteingaben.
Please optionally select an identifying letter for the new language	Weisen Sie der neuen Sprachversion einen Buchstaben zu.
Please upload the complete translation file for the new language	Wählen Sie die Ressourcendatei mit der kompletten Übersetzung für die neue Sprachversion zum Hochladen aus.

6.6.1.6 GINA Selbstregistrierung über Webmail Portal

Zum Registrieren eines eigenen GINA-Benutzerkontos ist es erforderlich, das GINA-Portal im Webbrowser aufzurufen. Sie gelangen über den folgenden Link zum GINA-Portal:

https://<IP-Adresse oder Hostname>/web.app

Externe Benutzer habe die Möglichkeit sich selbst über das GINA-Portal als GINA-Benutzer zu registrieren. Zum Selbstregistrieren eines externen Benutzers gehen Sie wie im Folgenden beschrieben vor:

Schritt 1

Registrieren Sie sich als GINA-Benutzer auf Ihrem SEPPmail System. Auf das GINA-Portal gelangen Sie via Webbrowser unter dem folgenden Link:

https://<SecureWebmailApplaince>/web.app

Der Platzhalter <SecureWebmailAppliance> steht für die IP-Adresse oder den Hostnamen unter der/dem das SEPPmail System intern erreichbar ist.

Damit der Bereich »Register new account« im GINA Secure Webmail-Portal angezeigt wird, muss im Menü »Mail Processing -> [Webmail-Domain]« in der Sektion »Extended Settings« die Option »Allow account self-registration in webmail without initial mail« aktiviert werden. Siehe GINA Webmail-Domains verwalten 69

Schritt 2

Wählen Sie im Bereich »Register new account« die Schaltfläche »Registration«, um ein Benutzerkonto anzulegen.

Wählen Sie die Schaltfläche »Continue« zu fortfahren. Bestätigen Sie im folgenden Dialog mit der Schaltfläche »Save«. Sie erhalten dann eine Bestätigungs-E-Mail mit einem »Activation-Link«. Mit der Auswahl dieses Links bestätigen Sie die Registrierung. Das Benutzerkonto ist nun aktiv und Sie können sich anmelden. Verwenden Sie dazu die bei der Registrierung angegebenen Daten für Benutzernamen und Passwort. (Benutzername = E-Mail Adresse)

Schritt 3

Bestätigen Sie den Activation-Link in der Bestätigungs-E-Mail.

Das neu angelegte GINA Konto wurde nun aktiviert und kann genutzt werden.

Schritt 4

Melden Sie sich hierzu mit Ihren Anmeldedaten an.

Nach der erfolgreichen Anmeldung an Ihren neuen GINA-Konto können Sie Ihr Konto verwalten oder eine neue GINA-Nachricht verfassen. Weitere Informationen erhalten Sie im Menü GINA Webmail Konto verwalten 81.

6.6.1.7 GINA Benutzerkonto verwalten

Zum Verwalten des eigenen GINA-Benutzerkontos ist es erforderlich, das GINA-Portal im Webbrowser aufzurufen. Sie gelangen über den folgenden Link zum GINA-Portal:

https://<IP-Adresse oder Hostname>/web.app

Zur Administration eines GINA-Benutzerkontos stehen die folgenden Schaltflächen zur Verfügung:

Write e-mail 81
Profile 81
Edit profile 81
Change password 81
Keys/Certificates 81

Schaltfläche »Write e-mail«

Wählen Sie die Schaltfläche »Write e-mail«, um eine neue GINA-Nachricht zu erzeugen. Als Absender wird Ihre eigene E-Mail-Adresse verwendet. Als Empfänger können Sie alle E-Mail-Adressen verwenden die im E-Mail-Routing des SEPPmail Systems eingerichtet sind. Hierbei handelt es sich um die internen E-Mail Adressen desjenigen, der das SEPPmail System betreibt.

Es ist nicht möglich, GINA-Nachrichten an beliebige externen Empfänger im Internet zu verwenden. Die Relayberechtigung gilt für alle internen E-Mail-Domains.

Schaltfläche »Profile«

Wählen Sie die Schaltfläche »Profile«, um die eigenen Profildaten anzuzeigen.

Schaltfläche »Edit profile«

Wählen Sie die Schaltfläche »Edit profile«, um die eigenen Profildaten zu ändern. Sie können die folgenden Daten ändern:

- Name
- Sprachvariante der Webmail Oberfläche
- Mobilfunkrufnummer

Schaltfläche »Change password«

Wählen Sie die Schaltfläche »Change password«, um das persönliche Kennwort und die Sicherheitsfrage zum Wiederherstellen eines Kennwortes zu ändern.

Schaltfläche »Keys/Certificates«

Wählen Sie die Schaltfläche »Keys/Certificates«, um eigene S/MIME Public Keys oder PGP Public Keys zum SEPPmail System hochzuladen. Diese Zertifikate und Schlüssel können zukünftig genutzt werden, um Ihnen S/MIME- oder PGP verschlüsselte E-Mails zu senden.

Ebenfalls haben Sie die Möglichkeit S/MIME oder PGP Public Keys von internen Mitarbeiten herunterzuladen, um diesen ebenfalls S/MIME- oder PGP verschlüsselte E-Mails zu senden.

6.6.1.8 GINA Self Service Passwort Management

Die Funktion »Self Service Passwort Management (SSPM)« ermöglicht es, dass vergessene Kennworte vom Empfänger automatisch und ohne Sicherheitsrisiken via Mobiltelefon neu generiert bzw. angefordert werden können.

Diese Funktion steht optional zur Verfügung. Sie benötigen dazu eine separate Lizenz. Ob Ihr SEPPmail System bereits für die Nutzung lizenziert ist können Sie im Menü »Home« in der Sektion » License« sehen.

Um diese Funktionen zu verwenden gehen Sie folgendermaßen vor:

Öffnen Sie eine bereits erhaltenen GINA-Nachricht. Im Anmeldedialog klicken Sie den »Forgot your Password?«

Sie erhalten daraufhin eine Auswahl der Möglichkeiten, wie Sie das Kennwort zurücksetzen können. In Abhängigkeit der Sicherheitseinstellungen für das Zurücksetzen des Kennworts werden Ihnen die folgenden Möglichkeiten angeboten:

Sie haben im Rahmen der Funktion »Self Service Passwort Management (SSPM)« zusätzlich zu den Standard-Funktionen folgende Möglichkeiten, das Kennwort zurückzusetzen:

Parameter	Beschreibung
default (Reset by hotline)	Standard Siehe GINA Webmail-Domains verwalten 72
Reset by Email verification	Standard Siehe GINA Webmail-Domains verwalten 72
Reset by hotline	Standard Siehe GINA Webmail-Domains verwalten 72
Reset by hotline, no reminder question/answer	Standard Siehe GINA Webmail-Domains verwalten 72

Diese folgenden Möglichkeiten für das Zurücksetzen eines Kennworts können nur im Rahmen der Funktion »Self Service Passwort Management (SSPM)« ausgeführt werden.

Parameter	Beschreibung
Reset by SMS	der Webmail-Benutzer erhält ein neues Kennwort via SMS, wenn die Sicherheitsfrage richtig beantwortet wurde, danach muss der Webmail-Benutzer ein neues Kennwort auswählen und speichern
Let user choose between hotline and SMS	der Webmail-Benutzer hat die Möglichkeit, dass Zurücksetzen des Kennworts zwischen der Option Hotline und SMS auszuwählen

6.6.1.9 GINA Interne Verschlüsselung

Die Funktion Interne Verschlüsselung (IME) ermöglicht es, dass auch firmenintern vertrauliche E-Mails auf komfortable Weise verschlüsselt versendet werden können – vom Arbeitsplatz des Absenders bis zum Desktop des Empfängers. Dadurch sind vertrauliche interne E-Mails im gesamten Firmennetz vor unerlaubtem Zugriff geschützt.

Diese Funktion steht optional zur Verfügung. Sie benötigen dazu eine separate Lizenz. Ob Ihr SEPPmail System bereits für die Nutzung lizenziert ist können Sie im Menü »Home« in der Sektion »License« sehen.

Um diese Funktionen zu verwenden gehen Sie folgendermaßen vor:

Schritt 1

Registrieren Sie sich als interner GINA-Benutzer auf Ihrem SEPPmail System. Auf das GINA-Portal gelangen Sie via Webbrowser unter dem folgenden Link:

https://<SecureWebmailApplaince>/web.app

Der Platzhalter <SecureWebmailAppliance> steht für die IP-Adresse oder den Hostnamen unter der/dem das SEPPmail-System intern erreichbar ist.

Damit der Bereich »Register new account« in der Webmail-Oberfläche angezeigt wird, muss im Menü »Mail Processing -> [Webmail-Domain]« in der Sektion »Extended Settings« die Option »Allow account self-registration in webmail without initial mail« aktiviert werden. Siehe GINA Webmail-Domains verwalten 69

Wählen Sie im Bereich »Register new account« die Schaltfläche »Registration«, um ein Benutzerkonto anzulegen.

Wählen Sie die Schaltfläche »Continue« zu fortfahren. Bestätigen Sie im folgenden Dialog mit der Schaltfläche »Save«. Sie erhalten dann eine Bestätigungs-E-Mail mit einem »Activation-Link«. Mit der Auswahl dieses Links bestätigen Sie die Registrierung. Das Benutzerkonto ist nun aktiv und Sie können sich anmelden. Verwenden Sie dazu die bei der Registrierung angegebenen Daten für Benutzernamen und Passwort. (Benutzername = E-Mail Adresse)

Schritt 2

Nach erfolgreichem Anmelden können Sie über ihr neues GINA-Konto E-Mails an interne Benutzer versenden. Der Empfänger erhält Ihre Nachricht als verschlüsselte GINA-Nachricht in sein Postfach. Die Nachricht bleibt auch nach dem Lesen weiterhin verschlüsselt im Postfach des Empfängers.

6.6.1.10 GINA S/MIME- und PGP Schlüsselsuche via GINA-Portal

Externe Benutzer habe die Möglichkeit über das GINA-Portal selbst nach S/MIME- oder PGP Public-Keys von internen Mitarbeitern suchen und diese herunterladen. Es ist ebenfalls möglich nach S/MIME- oder PGP Public-Keys von Zertifikaten für die Domainverschlüsselung zu suchen und diese herunterzuladen.

Zum GINA-Portal gelangen Sie via Webbrowser unter dem folgenden Link: https://<SecureWebmailApplaince>/web.app

Der Platzhalter <SecureWebmailAppliance> steht für die IP-Adresse oder den Hostnamen unter der/dem das SEPPmail System intern erreichbar ist.

Damit der Bereich »Search Keys/Certificates« im GINA-Portal angezeigt wird, muss im Menü »Mail Processing -> [Webmail-Domain]« in der Sektion » Extended Settings« der Parameter »Allow unregistered users to search public keys/certificates of internal users« aktiviert werden. Siehe GINA Webmail-Domains verwalten 69.

Damit der Bereich »Search Keys/Certificates« nur für angemeldete Benutzer angezeigt wird, muss die Option »Enable S/MIME certificate / PGP key search and management in webmail« aktiviert werden.

6.6.2 Regeln zur Verarbeitung von GINA-Nachrichten verwalten

Menü »Mail Processing« -> Sektion »GINA settings«

Parameter	Beschreibung
Password Length	Länge der durch Enhanced Secure Webmail automatisch generierten Kennworte (Standard: 8 Zeichen) (0 = Kennworte werden nicht automatisch generiert, sondern vom Empfänger der GINA-Nachricht gesetzt)
Use virtual hosting	Definiert das Aussehen der URL für den Zugang zum GINA-Portal beim hinzufügen zusätzlicher GINA-Domains
Secure GINA track access (e.g. http://192.168.1.60:8080)	Adresse der Web-Anwendung zur Anzeige des Lesestatus einer GINA-Nachricht

Im Standardverhalten verwendet GINA pro angelegter GINA-Domain eine eigenständige URL für den Zugang zum GINA-Portal.

```
Beispiel:

Es sind drei GINA-Domains angelegt. Jede GINA-Domain besitzt eine eigene
Portalkonfiguration. Auf die jeweiligen GINA-Portale kann über eine eigenständige
URL zugegriffen werden.

https://secmail.customer1.com/web.app
https://secmail.customer2.com/web.app
https://secmail.customer3.com/web.app
```

Die im Beispiel angegebenen FQDNs werden als Hostname innerhalb der jeweiligen GINA-Domain angegeben.

```
Beispiel:

Hostname: secmail.customer1.com
```

Das Standardverhalten kann durch den folgenden Parameter verändert werden.

Parameter »Use virtual hosting«

Die Aktivierung dieses Parameters ist erforderlich, wenn zusätzliche GINA-Domains angelegt werden müssen und das jeweilige GINA-Portal für die zusätzlichen Domains über eine eigenständige URL

erreichbar soll.

Standardverhalten ohne zusätzliche GINA-Domains und ohne aktiviertes »virtuelles Hosting«

```
Beispiel:

GINA-Hostname [Default]:
   secmail.customer.com

GINA-URL eingebettet in der Secure-Webmail [Default]:
   https://secmail.customer.com/web.app?op=init
```

Standardverhalten mit zusätzlichen GINA-Domains und ohne aktiviertes »virtuelles Hosting«

```
Beispiel:

GINA-Hostname [Default]:
   secmail.customer.com

GINA-URI eingebettet in der Secure-Webmail für [Default]:
   https://secmail.customer.com/web.app?op=init


GINA-Hostname [customerDomain1]:
   secmail.customer1.com

GINA-URI eingebettet in der Secure-Webmail für [customerDomain1]:
   https://secmail.customer.com/secmail.customer1.com/web.app?op=init
```

In diesem Beispiel können Sie erkennen, dass ohne »virtuelles Hosting« das GINA-Portal der zusätzlichen GINA-Domain als Pfad unterhalb der [Default] GINA-Domain verwendet wird. Um dieses Verhalten zu optimieren kann es sinnvoll sein, keinen separaten FQDN als Hostnamen für die zusätzliche Domain zu verwenden sondern einen einfachen Pfadnamen.

```
Beispiel:

GINA-Hostname [customerDomain1]:
   mypath

GINA-URI eingebettet in der Secure-Webmail für [customerDomain1]:
   https://secmail.customer.com/mypath/web.app?op=init

Ersetzen Sie den Pfad »mypath« durch einen für Sie passenden Wert.
```

Verhalten mit zusätzlichen GINA-Domains und MIT aktiviertem »virtuellen Hosting«

Bei aktiviertem »virtuellem Hosting« sind die GINA-Portale der zusätzlichen GINA-Domains über eine eigenständige URL erreichbar. Innerhalb jeder zusätzlichen GINA-Domain muss ein eindeutiger FQDN als Hostname eingetragen werden.

```
Beispiel:

GINA-Hostname [Default]:
```

```
   secmail.customer.com

GINA-URL eingebettet in der Secure-Webmail [Default]:
   https://secmail.customer.com/web.app?op=init


GINA-Hostname [customerDomain1]:
   secmail.customer1.com

GINA-URI eingebettet in der Secure-Webmail für [customerDomain1]:
   https://secmail.customer1.com/web.app?op=init
```

Parameter »Secure GINA track access«

Diese Funktion ermöglicht eine differenzierte Rückmeldung von Lesebestätigungen für versendete GINA-Nachrichten. Wird eine GINA-Nachricht mit Anforderung der Lesebestätigung an mehrere Empfänger verschickt, wird dem Absender nur die erste Lesebestätigung zurückgeschickt. Zusätzlich enthält die Lesebestätigung einen Link, unter dem die vollständige Übersicht der Lesebestätigungen aufgeführt ist. Dieser Link beginnt mit der Adresse, welche in diesem Feld eingegeben wird. Der hintere Teil des Links wird jeweils dynamisch generiert.

```
Beispiel:

http://192.168.1.60:8080

Rückmeldung an den Absender
http://192.168.253.60:8080/track.app?track=$MjAxMzA3Mj...
```

6.6.3 GINA-SMS Kennwortversand verwalten

Menü »Mail Processing« -> Sektion »GINA password via SMS«

Allgemeiner Hinweis zum SMS-Versand von GINA-Kennwortbenachrichtigungen

Die GINA-Schnittstelle ermöglicht es, beim erstmaligen Versand einer GINA-Nachricht, die Kennwortbenachrichtigung via SMS an den Empfänger zu übermitteln.

Dieser Vorgang kann vereinfacht werden, indem die Mobilfunkrufnummer für den Versand der Kennwortbenachrichtigung als Bestandteil des Betreff der GINA-Nachricht verwendet wird. Die Mobilfunkrufnummer wird vor dem Versand ins Internet aus dem Betreff durch SEPPmail entfernt.

Sie haben die folgenden Möglichkeiten die Kennwortbenachrichtigung via SMS zu übermitteln:

- als Bestandteil der E-Mail-Betreffzeile

  (mobile: +49123456789) oder (sms: +49123456789) im Betreff einfügen

```
Beispiel:

Betreff: Sichere E-Mail-Verschlüsselung (mobile: +49123456789)
Betreff: Sichere E-Mail-Verschlüsselung (sms: +49123456789)
```

- verwenden einer zuvor im GINA-Benutzerkonto hinterlegten Mobilfunkrufnummer

  Die im GINA-Benutzerkonto hinterlegte Mobilfunkrufnummer kann für die Funktion »Self-Service password management« verwendet werden. Externe GINA-Benutzer haben die Möglichkeit das eigene Benutzerkennwort bei Bedarf selbstständig zurückzusetzen.

- Senden eines Einmalkennworts (One-Time Password) über die Konfigurationsoberfläche im Menü »GINA accounts -> [Name des GINA-Benutzerkontos]«

  Diese Option wird i.d.R. zum Zurücksetzen des Benutzerkennworts durch einen Administrator verwendet.

- Verwenden einer in SEPPmail integrierten Web-Anwendung (Standard)

  Für den internen Benutzer kann eine integrierte Web-Anwendung zum SMS-Versand an neue externe GINA-Benutzer eingerichtet werden. Auf diese Web-Anwendung kann wahlweise über den Konfigurationswebserver oder das öffentliche GINA-Portal zugegriffen werden.

Zum Einrichten der Schnittstelle für den SMS-Versand stehen bei SEPPmail unterschiedliche Konfigurationsmöglichkeiten zur Verfügung. Hierbei handelt es sich um eine global wirksame Konfiguration die nicht durch den Benutzer beeinflusst werden kann.

Parameter	Beschreibung
Disable	SMS-Versand deaktivieren
Use cell phone / GSM modem attached to appliance	Mobiltelefon oder GSM-Modem verwenden, welches direkt an die Hardware-Appliance angeschlossen ist
Use Mail to SMS service (configuration below)	E-Mail-zu-SMS Dienst oder Gateway mit folgenden Einstellungen verwenden
Use xml service (configuration below)	XML-Dienst verwenden (weitere Informationen erhalten Sie über den technischen Support)
Use HTTP GET service (configuration below)	HTTP-GET-Dienst verwenden (weitere Informationen erhalten Sie über den technischen Support)

In Abhängigkeit der ausgewählten Option für den SMS-Versand können Sie die Detailkonfiguration vornehmen.

Die folgenden Variablen (Platzhalter) stehen innerhalb der Konfiguration für den XML-Dienst und den HTTP-GET-Dienst zur Verfügung:

1. `$sms` : zu übermittelnder Nachrichtentext
2. `$number` : Mobilfunkrufnummer incl. Landesvorwahl (+xx...)
3. `$countrycode` : Landesvorwahl, z.B. "49"
4. `$localnumber` : Mobilfunkrufnummer OHNE Landesvorwahl

Parameter »Use cell phone / GSM modem attached to appliance«

Für diesen Parameter steht keine Detailkonfiguration zur Verfügung. Bei Verwendung einer Hardware-Appliance haben die Möglichkeit, ein Mobiltelefon direkt via USB-Kabel anzuschließen. Die Steuerung erfolgt dabei automatisch durch das SEPPmail System.

Parameter »Use Mail to SMS service«

Mail from:
Absender Mail-Adresse für den SMS-Versand

Gateway Domain <Mobile #>@:
Gateway-Domäne für den SMS-Versand

Parameter »Use xml service«

Hier binden Sie den XML-Service eines externen Dienstleisters ein, um GINA-Kennwortbenachrichtigungen via SMS zu versenden. Dazu stehen die folgenden Parameter zur Verfügung:

Server address:
Adresse des externen Servers an den das XML-Template übermittelt werden soll. Sie erhalten diese Adresse von Ihrem Dienstleister.

```
XML-Beispiel: https://xml1.aspsms.com
```

xml template:
Quellcode für das XML-Template. Sie erhalten diese Daten von Ihrem Dienstleister.

```
XML-Beispiel:

<?xml version="1.0" encoding="UTF-8"?>
<aspsms>
      <Userkey>xyz</Userkey>
      <Password>xyz</Password>
      <Originator>Secmail</Originator>
      <FlashingSMS>1</FlashingSMS>
      <Recipient>
            <PhoneNumber>$number</PhoneNumber>
      </Recipient>
      <MessageData><![CDATA[$sms]]></MessageData>
      <Action>SendTextSMS</Action>
</aspsms>
```

Parameter »Use HTTP GET service«

Hier binden Sie den HTTP-GET-Service eines externen Dienstleisters ein, um GINA-Kennwortbenachrichtigungen via SMS zu versenden. Dazu stehen die folgenden Parameter zur Verfügung:

Server address:
Adresse des externen Servers an den der HTTP-GET-String übermittelt werden soll. Sie erhalten diese Adresse von Ihrem Dienstleister.

```
HTTP-Get-Beispiel: https://www.chrus.ch
```

HTTP Get String:

Pfadname mit Anwendung incl. der übergebenen Parameter mit den zu übermittelnden SMS-Daten.

```
HTTP-Get-Beispiel: /mysms/http/send.php?
user=xyz&pwd=xyz&from=Secmail&to=$number&msg=$sms
```

Zugriffsberechtigung auf die integrierte Web-Anwendung für den SMS-Versand

Parameter	Beschreibung
Disabled	Zugang zur Web-Anwendung für den SMS-Versand ist deaktiviert
Available via public GINA GUI	Aktiviert den Zugang zur Web-Anwendung für den SMS-Versand von Kennwortbenachrichtigungen über das öffentliche GINA-Portal. Die Web-Anwendung steht auf demselben Port zur Verfügung wie das GINA-Portal. (Standard: TCP/443 - HTTPS)
Available via the following URL (eg. https://192.168.1.60:8443/pwsend.app)	Aktiviert den Zugang zur Web-Anwendung für den SMS-Versand von Kennwortbenachrichtigungen aus dem internen Netzwerk. Die Web-Anwendung steht auf demselben Port zur Verfügung wie die Konfigurationsoberfläche. (Standard TCP/8443)

Access to GINA send password form:

Parameter »Available via public Webmail GUI«

Zum Versenden einer Kennwortbenachrichtigung via SMS erhält der interne Absender eine E-Mail-Nachricht. Diese Kennwortbenachrichtigung wird beim Erzeugen eines GINA-Kontos für einen externen Empfänger automatisch generiert und an den internen Absender gesendet. In dieser E-Mail-Nachricht befindet sich ein Link zu einer Web-Anwendung über die der SMS-Versand durchgeführt wird. Je nach individueller Implementierung des Enhanced Secure Webmail-Systems kann es erforderlich sein, auf diese Web-Anwendung über das öffentliche GINA-Portal zuzugreifen. Aktivieren Sie diese Option, um über den Port auf die Web-Anwendung zuzugreifen über auch das GINA-Portal erreichbar ist. Es wird empfohlen den Standard-Port für HTTPS (TCP/443) zu verwenden.

```
Beispiel:

GINA-Portal erreichbar über:
https://secmail.customer.com/web.app

Web-Anwendung für den SMS-Versand der Kennwortbenachrichtigung erreichbar über:
https://secmail.customer.com/pesend.app
```

Parameter »Available via the following URL«

Zum Versenden einer Kennwortbenachrichtigung via SMS erhält der interne Absender eine E-Mail-Nachricht. Diese Kennwortbenachrichtigung wird beim Erzeugen eines GINA-Kontos für einen externen Empfänger automatisch generiert und an den internen Absender gesendet. In dieser E-Mail-Nachricht befindet sich ein Link zu einer Web-Anwendung über die der SMS-Versand durchgeführt wird. Die Web-Anwendung ist ausschließlich über die in diesem Eingabefeld definierte URI erreichbar. Diese Einstellung können Sie verwenden, wenn die Web-Anwendung nur aus dem internen Netzwerk erreichbar sein soll.

```
Beispiel:
```

```
Web-Anwendung für den SMS-Versand der Kennwortbenachrichtigung erreichbar über:
https://192.168.1.60:8443/pwsend.app
```

6.6.4 Disclaimer verwalten

Menü »Mail Processing« -> Sektion »Edit Disclaimer«

Der Standard-Disclaimer hat die Bezeichnung [default]. Sie können neben dem Standard-Disclaimer zusätzliche Disclaimer hinzufügen und Konfigurieren, Disclaimer Löschen oder bestehende Disclaimer editieren.

Einen Disclaimer löschen

Um einen Disclaimer zu löschen, wählen Sie den zu löschenden Disclaimer aus und klicken Sie auf die Schaltfläche »Delete...«. Der Disclaimer wird aus der Konfiguration entfernt.

Beachten Sie dabei, dass dieser Disclaimer nicht mehr innerhalb der Ruleset-Programmierung wird, bevor Sie diesen löschen. Anderenfalls kann es zu Problemen bei der Ausführung von Ruleset-Anweisungen kommen.

Einen vorhandenen Disclaimer editieren

Um einen vorhandenen Disclaimer zu bearbeiten, klicken Sie die Schaltfläche »Edit...«.

Parameter »Disclaimer as text«

Fügen Sie in diesem Feld den Inhalt des Disclaimer im reinen Textformat ein.

Parameter »Disclaimer as Html«

Fügen Sie in diesem Feld den Inhalt des Disclaimers im HTML-Format ein. Sie können hier unterschiedliche HTML-Tags zur Formatierung benutzen. (z.B. Absätze, Schriftgröße oder Schriftfarbe)

Einen neuen Disclaimer erstellen

Sie können zusätzlich zum Standard-Disclaimer mit der Bezeichnung [default] bei Bedarf zusätzliche Disclaimer einrichten. Ein Disclaimer kann innerhalb der Konfiguration einer »Managed Domain« zugewiesen und verwendet werden. Der Disclaimer wird an alle ausgehenden E-Mails dieser »Managed Domain« automatisch angehängt.

Um einen zusätzlichen Disclaimer einzurichten, klicken Sie die Schaltfläche »Create new disclaimer...«. Geben Sie eine Bezeichnung für den neuen Disclaimer ein und klicken Sie die Schaltfläche »Create«. Wählen Sie anschließend Ihren neuen Disclaimer in der Auswahlliste aus und klicken Sie auf die Schaltfläche »Edit...«. Sie können nun den Text des neuen Disclaimers bearbeiten.

6.6.5 Mail-Vorlagen (Templates) verwalten

Menü »Mail Processing« -> Sektion »Edit Mail Templates«

Bei Templates handelt es sich um vordefinierte Nachrichten, welche in definierten Fällen automatisiert versendet werden. Templates können nur innerhalb von Ruleset-Anweisungen verwendet werden.

Das Standard-Template »bounce_noenc« verwalten

Das einzige Template, welches nach Inbetriebnahme der SEPPmail-Systems zur Verfügung steht, hat die Bezeichnung »bounce_noenc«. Dieses Template kommt zum Einsatz, wenn ein Absender versucht, eine verschlüsselte E-Mail zu verschicken, die Verschlüsselung jedoch fehlschlägt. Die E-Mail wird in einem solchen Fall nicht durch Enhanced Secure Webmail versendet. Der Absender erhält eine Benachrichtigung via E-Mail mit dem Inhalt des Templates als Nachrichtentext.

Um das Template »bounce_noenc« zu bearbeiten, klicken Sie auf die Schaltfläche »Edit...«.

Ein Template löschen

Um ein Template zu löschen, wählen Sie das zu löschende Template aus und klicken Sie auf die Schaltfläche »Delete...«. Das Template wird aus der Konfiguration entfernt.

Beachten Sie dabei, dass dieses Template nicht mehr innerhalb der Ruleset-Programmierung wird, bevor Sie es löschen. Anderenfalls kann es zu Problemen bei der Ausführung von Ruleset-Anweisungen kommen.

Ein bestehendes Template editieren

Um ein vorhandenes Template zu bearbeiten, klicken Sie die Schaltfläche »Edit...«.

Parameter »Template as text«

Fügen Sie in diesem Feld den Inhalt des Templates im Textformat ein.

Die folgenden Variablen (Platzhalter) stehen innerhalb der Konfiguration für das Template zur Verfügung:

1. $to : E-Mail-Adresse des Empfängers
2. $header_to : Header der ursprünglichen E-Mail als Anlage

Ein neues Template erstellen

Sie können zusätzlich zum Standard-Template mit der Bezeichnung »bounce_noenc« bei Bedarf zusätzliche Templates einrichten. Ein Template wird jeweils durch eine entsprechende Regelwerk-Anweisung verwendet.

Um ein zusätzliches Template einzurichten, klicken Sie die Schaltfläche »Create new template...«. Geben Sie eine Bezeichnung für das neue Template ein und klicken Sie die Schaltfläche »Create«. Wählen Sie anschließend Ihr neues Template in der Auswahlliste aus und klicken Sie auf die Schaltfläche »Edit...«. Sie können nun den Text des neuen Templates bearbeiten.

6.6.6 Regelwerk verwalten

Menü »Mail Processing« -> Sektion »Ruleset Generator«

Die Sektion »Ruleset« ist in folgende Bereiche unterteilt:

Diese Bereiche werden nachfolgend einzeln erläutert.

Sektion »Ruleset Generator« -> Bereich »General Settings«

Parameter	Beschreibung
Do not touch mails with the following text in subject	Definieren Sie einen Tag, um die cryptografische Verarbeitung einer E-Mail zu verhindern.
Add disclaimer to all outgoing emails	Fügt den Standard-Disclaimer allen ausgehenden E-Mail-Nachrichten hinzu.
Also add disclaimer to replies (in-reply-to header set)	Fügt den Standard-Disclaimer allen ausgehenden E-Mail-Nachrichten hinzu die durch den internen Benutzer als Antwort auf eine empfangene Nachricht gesendet wurden.
Reprocess mails sent to reprocess@decrypt.reprocess	Ermöglicht es, den Entschlüsselungsvorgang einer empfangenen E-Mail noch einmal durchzuführen.
Show message subject in logs	Aktiviert die Anzeige der Betreffzeile innerhalb der Log-Dateien.

Parameter »Do not touch mails with the following text in subject«

```
Standard: \[plain\]
```

Definieren Sie einen Tag, um die cryptografische Verarbeitung einer E-Mail zu verhindern. Fügen Sie diesen Tag incl. der eckigen Klammern in der Betreffzeile hinzu, so wird diese E-Mail durch das Ruleset nicht cryptografisch verarbeitet. Das Ruleset kann somit »umgangen« werden. Die Backslash innerhalb des Tags stellen Escape-Symbole dar. Dieses sind durch den Benutzer nicht einzugeben.

```
Beispiel:

Betreff: [plain] Sichere E-Mail-Verschlüsselung
```

Aktivieren Sie diesem Parameter, um dem Benutzer die Möglichkeit zu gehen das eingerichtete Ruleset zu umgehen.

Parameter »Add disclaimer to all outgoing mails«

Nutzen Sie diese Einstellung, wenn Sie den Standard-Disclaimer an alle ausgehenden E-Mail-Nachrichten anhängen möchten.

Parameter »Also add disclaimer to replies (in-reply-to header set)«

Nutzen Sie diese Einstellung, wenn Sie den Standard-Disclaimer auch an E-Mail-Nachrichten anhängen wollen auf die der interne Benutzer geantwortet hat.

Parameter »Reprocess mails sent to reprocess@decrypt.reprocess«

Diese Einstellung betrifft verschlüsselte E-Mails, die an interne E-Mail-Empfänger geschickt wurden und vom SEPPmail-System nicht entschlüsselt werden konnten. Dieser Fall kann z.B. eintreten, wenn das Secure-E-Mail-System zum Zeitpunkt des Erhalts einer E-Mail nicht über das benötigte Schlüsselmaterial verfügt. Mit diesem Parameter ermöglichen Sie entsprechenden Benutzern den Versand von E-Mails, welche nicht entschlüsselt werden konnten, an die Adresse »reprocess@decrypt.reprocess«, um den Entschlüsselungsvorgang mittels SEPPmail Appliance erneut auszulösen.

Parameter »Show message subject in logs«

Nutzen Sie diese Einstellung, wenn die Betreffzeile einer E-Mail in den Log-Dateien angezeigt werden soll.

Sektion »Ruleset« -> Bereich »User Creation«

Parameter	Beschreibung
Manual user creation: Only process outgoing mails from users with an account	Deaktiviert das automatische anlegen von Benutzerkonten.
automatically create accounts for new users if user tries to sign / encrypt	Aktiviert das automatische Anlegen von Benutzerkonten, wenn versucht wird die Cryptofunktionen zu nutzen.
automatically create accounts for all users	Aktiviert das automatische Anlegen von Benutzerkonten für alle internen Absender-E-Mail-Adressen, von denen E-Mails durch SEPPmail transportiert werden.

Parameter »Manual user creation: Only process outgoing mails from users with an account«

Aktivieren Sie diesen Parameter, wenn Sie die Nutzung der SEPPmail Appliance nur denjenigen Personen ermöglichen möchten, welche bereits über ein Benutzerkonto auf der Appliance verfügen.

Parameter »automatically create accounts for new users if user tries to sign / encrypt«

Dieser Parameter ermöglicht die automatische Erstellung neuer Benutzer. Ist diese Einstellung

aktiv, werden interne E-Mail-Absender automatisch als Benutzer auf der Appliance erfasst. Dies erfolgt dann, wenn der internen E-Mail-Absender versucht eine E-Mail zu signieren oder zu verschlüsseln.

Parameter »automatically create accounts for all users«

Dieser Parameter ermöglicht die automatische Erstellung neuer Benutzer. Ist diese Einstellung aktiv, werden interne E-Mail-Absender automatisch als Benutzer auf der Appliance erfasst.

Sektion »Ruleset« -> Bereich »Encryption / Decryption« -> »Incoming Emails«

Parameter	Beschreibung
Add this text to message subject after decryption	Definiert einen Tag, um eine erfolgreich entschlüsselte E-Mail zu markieren
Set confidential flag after decryption	Setzt die Outlook-Nachrichtenoption »vertraulich« nach erfolgreichen Entschlüsselung
Reject mails if S/MIME decryption fails	Zurückweisen von eingehenden S/MIME-verschlüsselten E-Mails die nicht erfolgreich entschlüsselt werden können

Parameter »Add this text to message subject after decryption«

```
Standard: \[secure\]
```

Sie können einen Tag definieren, um eine erfolgreich entschlüsselte E-Mail zu markieren. Dieser wird am Ende der Betreffzeile einer entschlüsselten E-Mail angehängt. Die Backslash innerhalb des Tags stellen Escape-Symbole für die öffnende und schließende eckige Klammer dar. Die Backslash werden beim Einfügen durch SEPPmail entfernt.

```
Beispiel:

Betreff: Sichere E-Mail-Verschlüsselung [secure]
```

Parameter »Set confidential flag after decryption«

Wird eine eingehende E-Mail durch SEPPmail entschlüsselt, so wird automatisch die Outlook-Nachrichtenoption »vertraulich« bei einer nach intern weitergeleiteten E-Mail gesetzt. Beim Antworten bleibt diese Nachrichtenoption erhalten und die ausgehende E-Mail wird durch SEPPmail ebenfalls verschlüsselt.

Parameter »Reject mails if S/MIME decryption fails«

Aktivieren Sie diesen Parameter, falls eingehende verschlüsselte E-Mails zurückgewiesen werden sollen, wenn die Entschlüsselung fehlschlägt.

Sektion »Ruleset« -> Bereich »Encryption / Decryption« -> »Outgoing Emails«

Parameter	Beschreibung
Always encrypt mails with the following text in subject	Ausgehende E-Mails werden verschlüsselt, wenn das angegebene Tag im Betreff eingefügt wurde.
Always encrypt mails with Outlook "confidential" flag set	Ausgehende E-Mails werden verschlüsselt, wenn die Microsoft-Outlook Nachrichtenoption "Vertraulich" gesetzt ist.
Always use GINA technology for mails with the following text in subject	Ausgehende E-Mails werden via GINA-Technologie verschlüsselt, wenn das angegebene Tag im Betreff eingefügt wurde.
Always use GINA technology for mails with Outlook "private" flag set	Ausgehende E-Mails werden via GINA-Technologie verschlüsselt, wenn die Microsoft-Outlook Nachrichtenoption "Privat" gesetzt ist.
Create GINA users with empty password if the following text is in the subject	Bei neu erzeugten GINA-Benutzerkonten wird ein leeres Kennwort gesetzt, wenn das angegebene Tag im Betreff eingefügt wurde.
Always use S/MIME or openPGP if keys are available	Ausgehende E-Mails werden automatisch S/MIME oder OpenPGP verschlüsselt, wenn Schlüsselmaterial des Empfängers im SEPPmail-Schlüsselspeicher vorhanden ist.
Always use GINA encryption if account exists and no S/MIME or openPGP key is known	Ausgehende E-Mails werden automatisch via GINA-Technologie verschlüsselt, wenn für den Empfänger ein GINA-Benutzerkonto existiert und kein Schlüsselmaterial des Empfängers im SEPPmail-Schlüsselspeicher vorhanden ist.
Do not encrypt outgoing mails with the following text in subject	Ausgehende E-Mails werden NICHT verschlüsselt, wenn das angegebene Tag im Betreff eingefügt wurde.

Parameter »Always encrypt mails with the following text in subject«

```
Standard: \[confidential\]
```

Sie können einen Tag definieren, um die Verschlüsselung einer ausgehenden E-Mail zu initiieren. Fügen Sie diesen Tag incl. der eckigen Klammern in der Betreffzeile hinzu, so wird SEPPmail diese E-Mail verschlüsselt versenden. Die passende Verschlüsselungsmethode wird dabei automatisch durch SEPPmail ausgewählt. Die Backslash innerhalb des Tags stellen Escape-Symbole dar. Dieses sind durch den Benutzer nicht einzugeben.

```
Beispiel:

Betreff: [confidential] Sichere E-Mail-Verschlüsselung
```

Reihenfolge der Verschlüsselungsmethoden

1. S/MIME-Benutzerverschlüsselung
2. PGP-Benutzerverschlüsselung

3. S/MIME-Domainverschlüsselung
4. PGP-Domainverschlüsselung
5. Verschlüsselung als GINA-Nachricht

Es wird versucht, die Verschlüsselungsmethoden der Reihenfolge nach anzuwenden. Wird kein Schlüsselmaterial des Empfängers im SEPPmail Schlüsselspeicher gefunden, so wird die E-Mail via Adhoc-Verschlüsselung als GINA-Nachricht versendet.

Wird die Verwendung der GINA-Technologie deaktiviert, und eine E-Mail kann nicht anderweitig verschlüsselt werden, so wird diese E-Mail von SEPPmail zurückgewiesen und nicht versendet. Der Absender erhält dazu eine E-Mail-Benachrichtigung. Es wird der Inhalt des Templates »bounce_noenc« verwendet.

Parameter »Always encrypt mails with Outlook "confidential" flag set«

Nutzen Sie diesen Parameter, wenn E-Mails in Microsoft-Outlook mit der Nachrichtenoption »Vertraulich« stets verschlüsselt werden sollen. Es wird analog zum vorherigen Menüpunkt verfahren.

Parameter »Always use secure webmail technology for mails with the following text in subject«

```
Standard: \[priv\]
```

Sie können einen Tag definieren, um die Verschlüsselung einer ausgehenden E-Mail via zu initiieren. Fügen Sie diesen Tag incl. der eckigen Klammern in der Betreffzeile hinzu, so wird SEPPmail diese E-Mail verschlüsselt versenden. Als Verschlüsselungsmethode wird die Verwendung der GINA-Technologie erzwungen. Die Backslash innerhalb des Tags stellen Escape-Symbole dar. Dieses sind durch den Benutzer nicht einzugeben.

```
Beispiel:

Betreff: [priv] Sichere E-Mail-Verschlüsselung
```

Parameter »Always use secure webmail technology for mails with Outlook "private" flag set«

Nutzen Sie diese Option, wenn E-Mails in Microsoft-Outlook mit der Nachrichtenoption »Private« stets verschlüsselt werden sollen. Als Verschlüsselungsmethode wird die Verwendung der GINA-Technologie erzwungen.

Parameter »Create Secure webmail users with empty password if the following text is in the subject«

```
Standard: \[emptypw\]
```

Sie können einen Tag definieren, um GINA-Benutzerkonten mit einem leeres Kennwort zu erzeugen. Fügen Sie diesen Tag incl. der eckigen Klammern in der Betreffzeile hinzu. Der Empfänger der GINA-Nachricht erhält kein Initialisierungskennwort. Er bestimmt sein persönlichen Kennwort beim erstmaligen Login innerhalb des GINA-Portals selbst. Die Backslash innerhalb des Tags stellen Escape-Symbole dar. Dieses sind durch den Benutzer nicht einzugeben.

```
Beispiel:

Betreff: [emptypw] Sichere E-Mail-Verschlüsselung
```

Parameter »Always use S/MIME or OpenPGP if keys are available«

Aktivieren Sie diesen Parameter, um ausgehende E-Mails via S/MIME oder OpenPGP zu verschlüsseln, sofern entsprechendes Schlüsselmaterial vom Empfänger im SEPPmail Schlüsselspeicher vorhanden sind. Bei vorhandenem Schlüsselmaterial des Empfängers erfolgt die Verschlüsselung nur dann, wenn für den internen Absender ein aktives Benutzerkonto existiert.

Parameter »Always use Webmail encryption if account exists«

Aktivieren Sie diesem Parameter, um ausgehende E-Mails immer als GINA-Nachricht zu versenden, falls für den Empfänger bereits ein GINA-Benutzerkonten existiert. Die Verwendung der GINA-Technologie wird für alle E-Mails an den Empfänger erzwungen.

Parameter »Do not encrypt outgoing mails with the following text in subject«

```
Standard: \[noenc\]
```

Sie können einen Tag definieren, um das Verschlüsseln einer ausgehenden E-Mail zu verhindern. Fügen Sie diesen Tag incl. der eckigen Klammern in der Betreffzeile hinzu, so wird diese E-Mail durch das Ruleset nicht cryptografisch verarbeitet. Das Ruleset kann somit »umgangen« werden. Die Backslash innerhalb des Tags stellen Escape-Symbole dar. Dieses sind durch den Benutzer nicht einzugeben.

```
Beispiel:

Betreff: [noenc] Sichere E-Mail-Verschlüsselung
```

Sektion »Ruleset« -> Bereich »Signing« -> »Incoming Emails«

Parameter	Beschreibung
Add this text to message subject if S/MIME signature check succeeds	Fügt eine Statusinformation im Betreff der E-Mail hinzu, wenn die S/MIME-Signaturprüfung erfolgreich durchgeführt werden konnte.
remove signature if S/MIME signature check succeeds	Entfernt die S/MIME-Signatur innerhalb der E-Mail, wenn die S/MIME-Signaturprüfung erfolgreich durchgeführt werden konnte.
Add this text to message subject if S/MIME signature fails	Fügt eine Statusinformation im Betreff der E-Mail hinzu, wenn die S/MIME-Signaturprüfung NICHT erfolgreich durchgeführt werden konnte.
remove signature if S/MIME signature check fails	Entfernt die S/MIME-Signatur innerhalb der E-Mail, wenn die S/MIME-Signaturprüfung NICHT erfolgreich durchgeführt werden konnte.

Parameter »Add this text to message subject if S/MIME signature check succeeds«

```
Standard: \[signed\sOK\]
```

Sie können einen Tag definieren, um eine S/MIME signierte E-Mail zu markieren deren Signatur erfolgreich geprüft werden konnte. Dieser Tag wird am Ende der Betreffzeile einer signierten E-Mail angehängt. Die Backslash innerhalb des Tags stellen Escape-Symbole für die öffnende und schließende eckige Klammer dar. Die Backslash werden beim Einfügen durch SEPPmail entfernt. Die S/MIME-Signatur wird gegen die Root-CA-Zertifikate im SEPPmail Zertifikatsspeicher (Menü »X.509 Root certificates«) geprüft. Bei der Prüfung werden nur Root-CA-Zertifikate mit dem Status »trusted« berücksichtigt.

```
Beispiel:

Betreff: Sichere E-Mail-Verschlüsselung [signed OK]
```

Parameter »remove signature if S/MIME signature check succeeds«

Aktivieren Sie diesen Parameter, falls Sie die S/MIME-Signatur einer E-Mail entfernen wollten. Dies wird nur ausgeführt, wenn die S/MIME-Signatur durch SEPPmail erfolgreich gegen eine Root-CA im eigenen Root-CA-Speicher geprüft werden konnte. (Siehe Menü »X.509 Root Certificates« 174)

Parameter »Add this text to message subject if S/MIME signature fails«

```
Standard: \[signed\sINVALID\]
```

Sie können einen Tag definieren, um eine S/MIME signierte E-Mail zu markieren deren Signatur NICHT erfolgreich geprüft werden konnte. Dieser Tag wird am Ende der Betreffzeile einer signierten E-Mail angehängt. Die Backslash innerhalb des Tags stellen Escape-Symbole für die öffnende und schließende eckige Klammer dar. Die Backslash werden beim Einfügen durch SEPPmail entfernt. Die S/MIME-Signatur wird gegen die Root-CA-Zertifikate im SEPPmail Zertifikatsspeicher (Menü »X.509 Root certificates«) geprüft. Bei der Prüfung werden nur Root-CA-Zertifikate mit dem Status »trusted« berücksichtigt.

```
Beispiel:

Betreff: Sichere E-Mail-Verschlüsselung [signed INVALID]
```

Parameter »remove signature if S/MIME signature check fails«

Aktivieren Sie diesen Parameter, falls Sie die S/MIME-Signatur einer E-Mail entfernen wollten. Dies wird nur ausgeführt, wenn die S/MIME-Signatur durch SEPPmail nicht erfolgreich gegen eine Root-CA im eigenen Root-CA-Speicher geprüft werden konnte. (Siehe Menü »X.509 Root Certificates« 174)

Sektion »Ruleset« -> Bereich »Signing« -> »Outgoing Emails«

Parameter	Beschreibung
S/MIME sign outgoing mails with the following text in subject	Ausgehende E-Mails werden S/MIME signiert, wenn das angegebene Tag im Betreff eingefügt wurde.

Parameter	Beschreibung
Sign all outgoing Emails if S/MIME certificate available	Ausgehende E-Mails werden S/MIME signiert, wenn für den internen Absender ein Benutzerkonto existiert und ein S/MIME-Zertifikat vorhanden ist.
Do not S/MIME sign outgoing mails with the following text in subject	Ausgehende E-Mails werden NICHT S/MIME signiert, wenn das angegebene Tag im Betreff eingefügt wurde.
S/MIME sign outgoing mails with domain key with the following text in subject	Ausgehende E-Mails werden S/MIME signiert, wenn das angegebene Tag im Betreff eingefügt wurde. Hierbei wird nicht das S/MIME Benutzerzertifikat des Absenders verwendet, sondern das Zertifikat eines durch die angegebene E-Mail definierten Benutzers.

Parameter »S/MIME sign outgoing mails with the following text in subject«

```
Standard: \[sign\]
```

Sie können einen Tag definieren, um eine ausgehende E-Mail zu signieren. Fügen Sie diesen Tag incl. der eckigen Klammern in der Betreffzeile hinzu. Falls ausgehende E-Mails nicht standardmäßig signiert werden, so kann der Benutzer die Signierung der aktuellen E-Mail initiieren. Die Backslash innerhalb des Tags stellen Escape-Symbole dar. Dieses sind durch den Benutzer nicht einzugeben.

```
Beispiel:

Betreff: [sign] Sichere E-Mail-Verschlüsselung
```

Parameter »Sign all outgoing Emails if S/MIME certificate available«

Aktivieren Sie diesem Parameter, um sämtliche ausgehenden E-Mails zu signiert, sofern ein entsprechende S/MIME-Zertifikat für den Absender vorhanden sind.

Parameter »Do not S/MIME sign outgoing mails with the following text in subject«

```
Standard: \[nosign\]
```

Sie können einen Tag definieren, um eine ausgehende E-Mail NICHT zu signieren. Fügen Sie diesen Tag incl. der eckigen Klammern in der Betreffzeile hinzu, so wird diese E-Mail durch das Ruleset nicht cryptografisch verarbeitet, falls dies evtl. der Voreinstellung entsprechen sollte. Das Ruleset kann somit »umgangen« werden. Die Backslash innerhalb des Tags stellen Escape-Symbole dar. Dieses sind durch den Benutzer nicht einzugeben. Die Backslash innerhalb des Tags stellen Escape-Symbole dar. Diese sind durch den Benutzer nicht einzugeben.

```
Beispiel:

Betreff: [nosign] Sichere E-Mail-Verschlüsselung
```

Parameter »S/MIME sign outgoing mails with domain key with the following text in subject«

```
Standard: \[domainsign\]
```

Sie können einen Tag definieren, um eine ausgehende E-Mails mit einem Domainzertifikat Ihrer Organisation zu signieren. Fügen Sie diesen Tag incl. der eckigen Klammern in der Betreffzeile hinzu. Falls ausgehende E-Mails nicht standardmäßig signiert werden, so kann der Benutzer die Signierung der aktuellen E-Mail initiieren. Die Backslash innerhalb des Tags stellen Escape-Symbole dar. Dieses sind durch den Benutzer nicht einzugeben.

```
Beispiel:

Betreff: [domainsign] Sichere E-Mail-Verschlüsselung
```

Weitere Konfigurationsparameter:

1. Using Certificate : zu verwendendes Domainzertifikat eines aus einem in SEPPmail
2. Text before new FROM : Text vor dem Domainabsender
3. Text after new FROM : Text nach dem Domainabsender

Sektion »Ruleset« -> Bereich »Key Generation«

Parameter	Beschreibung
automatically create openPGP keys for new users	automatisches Erzeugen von OpenPGP Benutzerschlüsseln
automatically create S/MIME keys for new users	automatisches Erzeugen von S/MIME Benutzerzertifikaten
automatically buy .... S/MIME keys for new users	automatisches Beziehen von S/MIME-Benutzerzertifikaten über den angezeigten CA-Connector

Parameter »automatically create openPGP keys for new users«

Dieser Parameter bewirkt, dass für neue Benutzer automatisch OpenPGP-Schlüssel erzeugt werden.

Parameter »automatically create S/MIME keys for new users«

Dieser Parameter bewirkt, dass für neue Benutzer automatisch S/MIME-Zertifikate erzeugt werden.

Parameter »automatically buy SwissSign S/MIME keys for new users«

Dieser Parameter ist im Standard nicht sichtbar. Er wird in Abhängigkeit des aktivierten CA-Connnectors angezeigt. Aktivieren Sie diesen, um automatisch Benutzerzertifikate für neue Benutzer über den jeweiligen CA-Connector zu beziehen.

Folgende CA-Connectoren stehen im Menü »CA« zur Verfügung:

1. S-TRUST : CA von Deutscher Sparkassen Verlag GmbH
2. none : CA-Connector ist deaktiviert
3. Signtrust : CA von Deutsche Post Signtrust und DMDA GmbH

4. SwissSign : CA von SwissSign AG (100%-ige Tochterfirma der Schweizerischen Post)

Sektion »Ruleset« -> Bereich »Protection Pack (Anti-SPAM / Anti-Virus)«

Parameter	Beschreibung
Check mails for viruses and send infected mails to (leave empty to reject infected mails)	Aktiviert den Virenscanner und sendet infizierte E-Mails an die angegebene E-Mail-Adresse.
Send notification to this email address if a virus was found	Sendet eine Benachrichtigung über einen Virenfund an die angegebene E-Mail-Adresse.
Check incoming mails for spam and add the following text to the subject to identify spam	Aktiviert die SPAM-Prüfung eingehender E-Mails und markiert diese nach erfolgreicher SPAM-Prüfung.
Check incoming mails for spam and redirect spam to (leave empty to reject spam)	Aktiviert die SPAM-Prüfung und sendet als SPAM erkannte E-Mails an die angegebene E-Mail-Adresse.

Parameter »Check mails for viruses and send infected mails to (leave empty to reject infected mails)«

Sie können mit diesem Parameter eingehende E-Mails auf Viren überprüfen und bei erkannter Infektion an die zusätzliche angegebene E-Mail-Adresse weiterleiten. Der ursprüngliche Empfänger erhält die infizierte E-Mail nicht. Wenn keine E-Mail-Adresse angegeben ist, werden entsprechende E-Mails gelöscht.

Parameter »Send notification to this email address if a virus was found«

Wird bei einer eingehenden E-Mail ein Virus gefunden, so wird eine Benachrichtigung über dieses Ereignis an die hier angegebene E-Mail-Adresse gesendet.

Parameter »Check incoming mails for spam and add the following text to the subject to identify spam«

```
Standard: [SPAM]
```

Sie können mit diesem Parameter eingehende E-Mails auf SPAM überprüfen. Handelt es sich um eine als SPAM erkannte E-Mail, so wird der zusätzlich definierte Tag am Ende der Betreffzeile hinzugefügt, um die E-Mail als SPAM gekennzeichnet.

Tag level: Sie definieren hier einen Schwellwert, ab dem eine eingehende E-Mail als SPAM eingestuft und markiert wird. Je niedriger dieser Wert ist, desto wahrscheinlicher ist es, dass eine E-Mail als SPAM erkannt wird. Gleichzeitig erhöht sich bei niedrigen Werten das Risiko einer Falscherkennung, so dass legitime E-Mails als SPAM erkannt werden. Eine als SPAM erkannte und markierte E-Mail wird an den ursprünglichen Empfänger weitergeleitet.

Parameter »Check incoming mails for spam and redirect spam to (leave empty to reject spam)«

Sie können mit diesem Parameter eingehende E-Mails auf SPAM überprüfen und bei positiver Erkennung an die hier zusätzlich angegebene E-Mail-Adresse weiterleiten. Der ursprüngliche Empfänger erhält diese E-Mail nicht mehr. Wenn keine E-Mail-Adresse angegeben ist, werden entsprechende E-Mails gelöscht.

Spam level: Sie definieren hier einen Schwellwert, ab dem eine eingehende E-Mail als SPAM eingestuft und an die angegebene E-Mail-Adresse weitergeleitet wird. Wenn keine E-Mail-Adresse angegeben ist, werden entsprechende E-Mails beim Empfang zurückgewiesen.

Sektion »Ruleset« -> Bereich »Header tagging«

Wird das SEPPmail-System zusammen mit anderen E-Mail verarbeitenden Systemen verwendet die darauf angewiesen sind, dass eingehende-, ausgehende, verschlüsselte- und entschlüsselte E-Mails eine spezielle Markierung erhalten, so können Sie diese Markierung durch selbst definierte »X-Header« abbilden. Ein zusätzliches E-Mail verarbeitendes System kann diese durch SEPPmail gesetzten »X-Header« auswerten und darauf reagieren. Ein Beispiel für ein zusätzliches E-Mail verarbeitendes System kann ein Data Loss Prevention (DLP) System sein.

Parameter	Beschreibung
Set header X-..... to value ..... For all incoming mails	X-Header und Wert für alle durch SEPPmail empfangenen E-Mails, z.B. von intern oder extern empfangene E-Mails.
Set header X-..... to value ..... For all outgoing mails	X-Header und Wert für alle durch SEPPmail gesendeten E-Mails, z.B. GINA-Nachrichten die durch GINA erzeugt werden oder Status-Nachrichten die durch SEPPmail erzeugt werden.
Set header X-..... to value ..... For all mails that have been encrypted	X-Header und Wert für alle durch SEPPmail verschlüsselten E-Mails
Set header X-..... to value ..... For all mails that have been decrypted	X-Header und Wert für alle durch SEPPmail entschlüsselten E-Mails

Sektion »Ruleset« -> Bereich »Archiving«

Parameter	Beschreibung
Send a copy of ALL emails to the following Address	Sämtliche durch SEPPmail transportierte E-Mails werden an die angegebene E-Mail-Adresse in Kopie gesendet.

Sektion »Ruleset« -> Bereich »Custom Commands«

Parameter	Beschreibung
Custom commands for incoming Email	Ruleset-Befehle für die Verarbeitung eingehender Nachrichten
Custom commands for outgoing Email	Ruleset-Befehle für die Verarbeitung ausgehender Nachrichten
Custom commands for User Creation	Ruleset-Befehle für die Erstellung von Benutzerkonten

Diese zusätzlichen selbstdefinierten Ruleset-Befehle werden jeweils am Anfang der entsprechenden Sektion im Ruleset-Quellcode eingefügt und somit als erstes verarbeitet.

Parameter »Custom commands for incoming Email«

Nutzen Sie diesen Bereich, um zusätzliche selbstdefinierte Ruleset-Befehle für die Verarbeitung eingehender Nachrichten zu aktivieren.

Parameter »Custom commands for outgoing Email«

Nutzen Sie diesen Bereich, um zusätzliche selbstdefinierte Ruleset-Befehle für die Verarbeitung ausgehender Nachrichten zu aktivieren.

Parameter »Custom commands for User Creation«

Verwenden Sie diesen Bereich, um zusätzliche selbstdefinierte Ruleset-Befehle für die Erstellung von Benutzerkonten zu aktivieren.

Beispiel:

```
if (authenticated()) {
} else {
   createaccount('@CREATEGPGKEYS@');
   log(1, 'user account generated');
}
$?$
```

Sektion »Ruleset« -> Bereich »Advanced Options«

Parameter	Beschreibung
Re-inject mails to sending mailserver (use with care!)	Verarbeitete E-Mails werden an den einliefernden E-Mail-Server zurückgesendet
Run in queueless mode (use with care!)	Aktiviert den Queueless Mode für die Verarbeitung von E-Mail
Completely disable GINA technology	Deaktiviert das GINA-Subsystem

Parameter	Beschreibung
Completely disable user-based S/MIME and openPGP	Deaktiviert die benutzerbasierte S/MIME und OpenPGP Ver- und Entschlüsselung

Parameter »Re-inject mails to sending mailserver (use with care!)«

Mit dieser Einstellung werden alle E-Mails nach der Bearbeitung an den Server zurückgeschickt, von dem sie an SEPPmail gesendet wurden (z.B. zentrale E-Mail-Drehscheibe).

Parameter »Run in queueless mode (use with care!)«

Diese Einstellung bewirkt, dass E-Mails an einzelne Empfänger während der Verarbeitung nicht »zwischengespeichert« werden. Stattdessen wird die Verbindung einer eingelieferten E-Mail erst dann quittiert, wenn die verarbeitete E-Mail erfolgreich an den nächsten E-Mail-Server weitergeleitet wurde und diese abgehende Verbindung quittiert wurde. Wenn beim Versand an mehrere Empfänger die Annahme für einige Empfänger nicht quittiert wird, befinden sich diese E-Mails kurzzeitig bis zur Quittierung durch die empfangenden E-Mail-Server auf der Appliance.

Parameter »Completely disable secure webmail technology«

Mit dieser Option können Sie die GINA-Technologie zentral deaktivieren. Dies kann erforderlich sein, wenn SEPPmail von extern nicht erreichbar ist bzw. die GINA-Technologie nicht benötigt wird.

Parameter »Completely disable user-based S/MIME and openPGP«

Mit diesem Parameter können Sie die Benutzerverschlüsselung für S/MIME und OpenPGP zentral deaktivieren. Dies kann erforderlich sein, wenn Sie ausschließlich die GINA-Technologie oder ausschließlich Domainverschlüsselung nutzen wollen.

Sektion »Ruleset« -> Bereich »Advanced Options« -> »Remote GINA Relay«

Parameter	Beschreibung
Use remote GINA server, reachable under the following email address	E-Mail-Adresse des Remote GINA Servers
This is a remote GINA server	Konfigurationsparameter, wenn Sie SEPPmail als Remote GINA Relay nutzen

Um die GINA-Technologie nutzen zu können ist es erforderlich, dass SEPPmail-System aus dem Internet zu erreichen. Sollte dies nicht möglich sein, können Sie die GINA-Technologie nicht nutzen. Um diesem Umstand zu umgehen, können Sie ein externes SEPPmail-System als Remote GINA Relay nutzen.

Parameter »Use remote GINA server, reachable under the following email address«

Die Kommunikation zwischen dem internen SEPPmail und dem SEPPmail welches als Remote GINA Relay genutzt wird, erfolgt via E-Mail. Geben Sie die E-Mail-Adresse an, die für die

Kommunikation verwendet werden soll.

SEPPmail stellt in diesem Fall keine GINA-Funktionalität zur Verfügung, sondern leitet ausgehende E-Mails die via GINA-Technologie versendet werden sollen an das Remote GINA Relay weiter. In diesem Fall tragen Sie keine Werte für die Parameter unter »This is a remote Webmail server« ein.

Parameter »This is a remote GINA server«

Nutzen Sie SEPPmail als Remote GINA Relay, dann erfassen Sie die Werte für die folgenden Parameter. Tragen Sie für den Parameter »Use remote GINA server, reachable under the following email address« keinen Wert ein.

Relay for domain
E-Mail-Domain(s) des GINA-Absenders. Für die angegebenen E-Mail-Domain(s) stellt dieses System die GINA-Funktion nach extern bereit. Dieses System erzeugt GINA-E-Mails und stellt das Portal für die externen Benutzer zur Entschlüsselung bereit.

Relay email address
E-Mail-Adresse des Remote GINA Relay. Unter dieser E-Mail-Adresse ist dieses System als Remote GINA Relay erreichbar.

Relay domain key fingerprint
Fingerprint des Domainkeys welcher von diesem Relay-Server verwendet wird.

6.6.7 Regelwerk anzeigen und laden

Menü »Mail Processing« -> Sektion »SMTP Ruleset«

Paramerter	Beschreibung
Display	Zeigt das aktuelle Ruleset an.
Upload	Ermöglicht den Upload eines eigenen Rulesets.

6.7 Menüpunkt "SSL"

Wählen Sie den Menüpunkt »SSL«, um das SSL-Device-Zertifikat (Secure Sockets Layer) der SEPPmail Appliance zu verwalten.

Folgende Vorgänge werden in den kommenden Abschnitten beschrieben:

SSL-Device-Zertifikat selbst erstellen 106
SSL-Device-Zertifikat von einer öffentlichen Zertifizierungsstelle anfordern 108
Bestehendes SSL-Device-Zertifikat verwenden 109
SSL-Device-Zertifikat sichern 110

6.7.1 SSL-Device-Zertifikat selbst erstellen

Menü »SSL« -> Schaltfläche »Request an new Certificate...«

SEPPmail ermöglicht es, ein eigenes SSL-Device-Zertifikate über die Konfigurationsoberfläche zu erstellen. Für eine Testinstallation ist es nicht zwingend erforderlich ein kostenpflichtiges SSL-Device-Zertifikat zu beschaffen. Das Zertifikat kann auf der SEPPmail-Appliance automatisch generiert und signiert werden.

Füllen Sie die Felder wie folgt aus (die kursiven Felder müssen ausgefüllt werden):

Sektion »Issue To«

Parameter	Beschreibung
Name or IP (CN)	IP-Adresse oder Hostname unter der SEPPmail aus dem Internet erreichbar ist. Bei einem selbstsignierten Zertifikat muss der hier angegebene Werte dem Namen in der URL entsprechen unter der SEPPmail angesprochen wird. **Beispiel:** Soll SEPPmail unter der URL »**https://securewebmail.example.tld**« angesprochen werden, so lautet der im Feld »**Name or IP (CN)**« anzugebende Hostname »**securewebmail.example.tld**«.
E-Mail	Eine gültige E-Mail-Adresse innerhalb der Firma, unter der eine zuständige Person erreicht werden kann.
Org. Unit (OU)	Name der zuständigen Organisationseinheit (optional).
Organization (O)	Name der Organisation (optional).
Locality (L)	Ort, in dem die Organisation ihren Sitz hat (optional).
State (ST)	Kanton/Bundesland, in dem die Organisation ihren Sitz hat (optional).

Parameter	Beschreibung
Country (C)	Land, in dem die Organisation ihren Sitz hat.

Sektion »Attributes«

Parameter	Beschreibung
Key size (bits)	Schlüssellänge in Bits Mögliche Werte: 1024 oder 2048 Wählen Sie als Schlüssellänge immer den Wert »2048«. Kürzere Schlüssel gelten nicht mehr als ausreichend sicher.
Signature	Für diesen Parameter stehen die folgenden Werte zur Auswahl: »Create Certificate signing request«: Erzeugt einen Zertifikatsantrag (CSR) zum Signieren von einer öffentlichen Zertifizierungsstelle. »Create self-signed certificate«: Erzeugt ein selbstsigniertes SSL-Device-Zertifikat. Wählen Sie »Create self-signed certificate« aus, um ein selbst generiertes und selbst signiertes SSL-Device-Zertifikat zu erzeugen.

Um die Erstellung des SSL-Zertifikats auszuführen, klicken Sie auf die Schaltfläche »Create Request«. Danach erhalten Sie eine Bestätigung mit den Zertifikatsdetails.

Es ist ebenfalls möglich ein Wildcard SSL-Zertifikat zu erstellen. Wildcard Zertifikate gelten nicht nur für einen dedizierten Host sondern können für mehrere Hosts einer Domain verwendet werden.

Beispiel: Ein SSL-Zertifikat mit dem Namen ginatest.testdomain.net kann nur für diesen einen Host verwendet werden. Anderenfalls wird eine Zertifikatsfehlermeldung im Webbrowser angezeigt. Ein Wildcard SSL-Zertifikat können Sie auf beliebigen Hosts einer Domain verwenden, z.B. ginatest.testdomain.net, webmail.testdomain.net oder secmail.testdomain.net.

Um ein Wildcard SSL-Zertifikat zu erzeugen, geben Sie den Hostnamen wie folgt ein: *.kundendomain.tld .

Nach Eingabe der Informationen erhalten Sie eine Bestätigung mit den Zertifikatsdetails. Diese

beinhaltet neben den von Ihnen angegebenen Werten folgende Angaben:

1. die Seriennummer des Zertifikats (Serial No.)
2. die Gültigkeitsdauer (Validity)
3. den Fingerprint (SHA1 Fingerprint)

Bitte beachten Sie, dass zur Aktivierung des neuen SSL-Device-Zertifikats ein Neustart der SEPPmail-Appliance erforderlich ist. Sie können den Neustart ausführen, indem Sie im Menüpunkt »Administration« auf die Schaltfläche »Reboot« klicken und danach den angezeigten Sicherheitscode bestätigen.

6.7.2 SSL-Device-Zertifikat von einer öffentlichen Zertifizierungsstelle anfordern

Menü »SSL« -> Schaltfläche »Request an new Certificate...«

Gehen Sie wie folgt vor:

1. Verfahren Sie analog den Schritten im Abschnitt SSL-Device-Zertifikat selbst erstellen 106, wählen Sie jedoch für den Parameter »Signature« den Wert »Create Certificate signing request«, um einen Zertifikatsantrag (CSR) zu erstellen. Zum Erstellen des Zertifikatsantrags wählen Sie die Schaltfäche »Create Request«.

2. Wählen Sie die Schaltfläche »Download and Import signed Certificate...«.

> **Hinweis:**
>
> Falls Sie im oberen Bereich des Menüs die gelb hinterlegte Information **»Remember to import the signed certificate.«** angezeigt wird, so wurde zuvor bereits ein Zertifikatsantrag erstellt.

3. Kopieren Sie den Text in der Sektion »Request« und übermitteln Sie diesen an die Zertifizierungsstelle, von der Sie das SSL-Device-Zertifikat anfordern wollen. Sie sollten diesen Zertifikatsantrag zur Sicherheit noch einmal lokal in einer Textdatei speichern. Bei vielen Zertifizierungsstellen können Sie den Zertifikatsantrag (CSR) im Webportal bei der Beauftragung des SSL-Device-Zertifikats mit einfügen.

4. Sobald Sie von der Zertifizierungsstelle Ihr SSL-Device-Zertifikat erhalten haben, wählen Sie im Menü »SSL« die Schaltfläche »Download and Import signed Certificate...«

5. Fügen Sie das Zertifikat in der Sektion »Import Certificate« ein und wählen Sie dann die Schaltfläche »Import Certificate«. Der Vorgang zum Erstellen eines neuen SSL-Device-Zertifikats für die SEPPmail Appliance ist nun abbeschlossen. Zum Aktivieren des neuen SSL.Device-Zertifikats führen Sie bitte einen Neustart des SEPPmail Systems durch.

> **Hinweis:**
>
> Fügen Sie das neu erstellte eigene SSL-Device-Zertifikat zusammen mit den zusätzlich benötigten Zertifikaten für ein oder mehrere Intermediate CA-Zertifikate und das Zertifikat der Root-CA selbst in der dargestellten Reinhenfolge ein. Stellen Sie dabei sicher, dass die Reihenfolge in der die Zertifikatsbestandteile eingefügt werden korrekt ist. Sie können im Fehlerfall das SSL-Device-Zertifikat nicht nutzen. Ebenfalls kann es zu Problemen beim Zugriff auf die Konfigurationsoberfläche kommen. In diesem Fall können Sie die

```
Konfigurationsoberfläche über das Protokoll HTTP auf Port TCP/8080 erreichen.
(http://<Appliance>:8080)
```

Reihenfolge für das Einfügen der Zertifikatsbestandteile:

1. Public Key des eigenen SSL-Device-Zertifikats

2. Public Key von einer oder mehreren Intermediate CA-Zertifikaten

3. Public Key der Root-CA

6.7.3 Bestehendes SSL-Device-Zertifikat verwenden

Menü »SSL« -> Schaltfläche »Request an new Certificate...«

Sektion »Upload existing key«

Parameter	Beschreibung
X.509 Key	Fügen Sie den private-Key des Zertifikats ein.
X.509 Certificate	Fügen Sie den public-Key des Zertifikats ein.

Parameter »X.509 Key«

Fügen Sie in diesem Feld den private-Key des Zertifikats ein. Falls der private-Key durch ein Kennwort geschützt ist, muss dieses zuvor entfernt werden.

Parameter »X.509 Certificate (and optional intermediate certificates)«

Fügen Sie in diesem Feld den public-Key des Zertifikats ein. Zusätzlich zum eigenen public-Key fügen Sie hier ebenfalls weitere optionale Zweischenzertifikate (Intermediate Certificates) und den public-Key des Root-CA-Zertifikats ein. Draus ergibt sich eine Zertifikatskette (Chain) die der SEPPmail-Webserver an den Webbrowser des Benutzers übergibt und die zur Überprüfung des SSL-Device-Zertifikats verwendet werden.

Reihenfolge für das Einfügen der Zertifikatsbestandteile:

1. Public Key des eigenen SSL-Device-Zertifikats

2. Public Key von einer oder mehreren Intermediate CA-Zertifikaten

3. Public Key der Root-CA

Schließen Sie den Vorgang in beiden Fällen ab, indem Sie auf die Schaltfläche »Create Request« klicken.

6.7.4 SSL-Device-Zertifikat sichern

Menü »SSL« -> Schaltfläche »Backup Certificate«

Sichern Sie das Zertifikat, indem Sie auf die Schaltfläche »Backup Certificate« klicken. Sie können das aktuell installierte SSL-Device-Zertifikat (public- und private-Key) als Datei auf der lokalen Festplatte sichern. Die Zertifikatsdatei ist im PEM-Format und hat als Vorgabewert den Namen »cert.pem«.

Beispiel:

```
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQDqLer/5Tp0j/+v
.
.
.
KHp36xzcsUNklzcPW89MWdUccLKmMf+KTDQBaJqrHplhSgtkKLh+MdyzTCEgkldT
VFbcif6/k5dNnDxz/wCZSzQ=
-----END PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIFIjCCBAqgAwIBAgIJALbNmR60XAsAMA0GCSqGSIb3DQEBBQUAMIGmMRcwFQYD
.
.
.
7ej1ce+YN2vIn2mYMFtn0D+yCxP9mPLsAGEdO6EaY/IPRaVNJUI8XYmJSicyOzIY
PCqvmnfimMsxA3u0rID+ein0SwbR+g==
-----END CERTIFICATE-----
```

6.8 Menüpunkt "CA"

Wählen Sie den Menüpunkt »CA«, um die eigene Certificate Authority (CA) der SEPPmail Appliance zu verwalten.

Folgende Vorgänge werden in den kommenden Abschnitten beschrieben:

6.8.1 Interne CA-Einstellungen verwalten

Menü »CA«

Sektion »Certificate Revocation List«

Parameter »Certificate Revocation List (CRL) herunterladen«

Klicken Sie auf die Schaltfläche »Create and Download CRL«, um die CRL herunterzuladen und einzusehen. Die CRL-Datei kann unter der folgenden Adresse direkt vom SEPPmail-Webserver heruntergeladen werden:

https://<IP-Adresse-SEPPmail>/certs.crl

Sektion »Internal CA Settings«

Passen Sie die Einstellungen der internen CA den Angaben Ihrer Organisation an. Die angegebenen Werte werden beim Erzeugen von Zertifikaten durch die lokale SEPPmail-CA berücksichtigt.

Paramater »Static Subject Part«

C : Land, in dem die Organisation ihren Sitz hat
OU : Name der zuständigen Organisationseinheit
O : Name der Organisation

Parameter »Validity in days«

Gültigkeit des CA-Zertifikats in Tagen

Parameter »Extension settings« -> Bereich »Weitere Parameter«

name : Name des Parameters
value : entsprechender Wert

Beispiel:

SEPPmail unterstützt als Standardfunktion das Ausstellen und Bereitstellen einer CRL als Datei zum Download von extern. Um wirksam zu werden ist es erforderlich, den Sperrlistenverteilungspunkt im Zertifikat selbst mit anzugeben.

```
Fügen Sie dazu folgenden zusätzlichen Parameter hinzu:

name      : crlDistributionPoints
value     : URI:https://<Hostname SEPPmail>/certs.crl
```

Sektion »External CA«

Aktivieren Sie einen der vorhandenen CA-Connectoren, um automatisch Benutzerzertifikate über die Managed-PKI einer externen CA zu beziehen. Bei einer Managed-PKI handelt es sich um die Schnittstelle zu einem Zertifikatsanbieter der es ermöglicht, automatisiert Zertifikate abzurufen. Dazu ist i.d.R. eine vertragliche Vereinbarung mit dem ausgewählten Zertifikatsanbieter erforderlich. Der Folgende Zertifikatsanbieter Signtrust bietet hierzu einen sehr einfach zu handhabenden Online-Antrag an.

Sie können den Signtrust Online-Antrag unter diesem Link erreichen: Signtrust Online-Antrag

Folgende CA-Connectoren stehen im Menü »CA« zur Verfügung:

1. S-TRUST : CA von Deutscher Sparkassen Verlag GmbH
2. none : CA-Connector ist deaktiviert
3. Signtrust : CA von Deutsche Post Signtrust und DMDA GmbH
4. SwissSign : CA von SwissSign AG (100%-ige Tochterfirma der Schweizerischen Post)

6.8.2 CA-Zertifikat einrichten

Menü »CA«

Um ein CA-Zertifikat zu erzeugen, klicken Sie auf die Schaltfläche »Request a new Certificate...«. Gehen Sie bei der Zertifikatserstellung analog den Schritten im Kapitel SSL-Zertifikat einrichten 106 vor.

6.8.3 CA-Zertifikat sichern

Menü »CA«

Führen Sie die Sicherung aus, indem Sie auf die Schaltflächen »Download Certificate« und »Download Key« klicken.

Schaltfläche	Beschreibung
»Download Certificate«	Sichern Sie den öffentlichen Teil (public Key) des CA-Zertifikats.
»Download Key«	Sichern Sie den privaten Teil (private Key) des CA-Zertifikats.

6.8.4 Verbindung zur externen CA S-Trust einrichten

Menü »CA«

Um die Verbindung zum externen Zertifikatsanbieter S-Trust einzurichten, klicken Sie in der Konfigurationsoberfläche auf die Schaltfläche »Save«. Klicken Sie auf die Schaltfläche »S-Trust

connector...«, um die Einstellungen für die Einbindung der S-Trust MPKI zu bearbeiten.

Sollten Sie noch keinen CA-Connector eingerichtet haben, wählen Sie einen CA-Connector S-Trust aus und speichern Sie diese Einstellung. Jetzt können Sie den zuvor ausgewählten CA-Connector konfigurieren.

Alle zur Konfiguration erforderlichen Daten erhalten Sie von der S-Trust CA.

6.8.5 Verbindung zur externen CA Signtrust einrichten

Menü »CA«

Um die Verbindung zum externen Zertifikatsanbieter Signtrust einzurichten, klicken Sie in der Konfigurationsoberfläche auf die Schaltfläche »Save«. Klicken Sie auf die Schaltfläche »Signtrust connector...«, um die Einstellungen für die Einbindung der Signtrust MPKI zu bearbeiten.

Sollten Sie noch keinen CA-Connector eingerichtet haben, wählen Sie einen CA-Connector Signtrust aus und speichern Sie diese Einstellung. Jetzt können Sie den zuvor ausgewählten CA-Connector konfigurieren.

Alle zur Konfiguration erforderlichen Daten erhalten Sie von der Signtrust CA.

Parameter	Beschreibung
Certificate Request Sender Email	E-Mail Adresse die als Absender für die Beauftragung von Zertifikaten verwendet wird.
Class 3 certificate	Auswahl des Class3-Zertifikats zur persönlichen Identifizierung des Administrators.
Password	Kennwort für das Class3-Zertifikat des Administrators.

Hinweis:

Bitte beachten Sie, dass alle von SEPPmail an die CA ausgehenden E-Mails und alle von der CA zurück gesendeten E-Mails nicht durch einen vorgelagerten SPAM-Filter verändert, zurückgehalten oder gelöscht werden. Definieren Sie dazu bitte innerhalb den von Ihnen eingesetzten SPAM-Filters die entsprechenden Ausnahmen für die im Parameter Certificate Request Sender Email eingetragene E-Mail Adresse und für die von der CA als Absender verwendeten E-Mail Adresse stcertreq@support.signtrust.de.

Zur Nutzung des Signtrust CA-Connectors steht Ihnen der folgende Online-Anftrag zur Verfügung.

Der Bezug von Benutzerzertifikaten über den Signtrust CA-Connector erfolgt im Benutzerkonto im Menü »Users«.

6.8.6 Verbindung zur externen CA SwissSign einrichten

Menü »CA«

Um die Verbindung zum externen Zertifikatsanbieter SwissSign einzurichten, klicken Sie in der Konfigurationsoberfläche auf die Schaltfläche »Save«. Klicken Sie auf die Schaltfläche » SwissSign connector...«, um die Einstellungen für die Einbindung der SwissSign MPKI zu bearbeiten.

Sollten Sie noch keinen CA-Connector eingerichtet haben, wählen Sie einen CA-Connector SwissSign aus und speichern Sie diese Einstellung. Jetzt können Sie den zuvor ausgewählten CA-Connector konfigurieren.

Sie haben die Auswahl zwischen Silver light certificates oder Standard certificates. Um Silver light certificates zu verwenden, sind keine weiteren Angaben notwendig.

Alle zur Konfiguration erforderlichen Daten erhalten Sie von der SwissSign CA.

6.9 Menüpunkt "Administration"

Wählen Sie den Menüpunkt »Administration«, um administrative Aufgaben der SEPPmail-Appliance zu verwalten.

Folgende Vorgänge werden in den kommenden Abschnitten beschrieben:

6.9.1 SEPPmail Appliance registrieren

Menü »Administration« -> Sektion »License and Registration«

Eine Registrierung des SEPPmail-Systems ist erforderlich, um eine permanente Lizenz zu erhalten.

Klicken auf die Schaltfläche »Register this device...« und Sie erhalten Sie ein Registrierungsfenster. Füllen Sie die Felder im Registrierungsfenster mit Ihren Angaben aus. Geben Sie in der oberen Hälfte Ihre Kundeninformationen und in der unteren Hälfte die Daten Ihres Resellers ein. Schließen Sie die Eingaben ab, indem Sie auf die Schaltfläche »Send« klicken.

Erscheint die Meldung »Registration successful«, haben Sie den Registrierungsvorgang erfolgreich abgeschlossen.

Für diese Installation wird nun durch SEPPmail eine Lizenz für Ihr System ausgestellt. Der Import der Lizenz in SEPPmail erfolgt dabei automatisch durch eine Onlineverbindung zum Lizenzserver.

Für die Registrierung und den Lizenzbezug ist es erforderlich, dass SEPPmail eine Onlineverbindung ins Internet auf Zielport TCP/22 (SSH) herstellen kann. Sollte dies nicht möglich sein, so schlagen die Registrierung bzw. der Lizenzbezug fehl.

6.9.2 Lizenzdatei einspielen

Menü »Administration« -> Sektion »License and Registration«

Die Lizenzierung der SEPPmail-Appliance erfolgt nach kurzer Zeit automatisch, wenn Sie die Appliance registrieren (siehe Abschnitt Appliance registrieren 115).

Um eine Lizenzdatei manuell einzuspielen, klicken Sie auf die Schaltfläche »Import License File...«. Klicken Sie auf die Schaltfläche »Browse«, um die Lizenzdatei auszuwählen, welche Sie einspielen möchten.

Sie können die aktuellen Lizenzdaten im Menü »Home« einsehen.

Die Verwendung von Lizenzdateien wird für Neuinstallationen nicht mehr unterstützt. Bei Neuinstallationen erfolgt die Lizenzierung ausschließlich über die Onlinelizenzierung.

6.9.3 Appliance nach verfügbaren Updates prüfen

Menü »Administration« -> Sektion »Update«

Um Ihre SEPPmail-Appliance auf den neusten Softwarestand zu bringen, stehen in der Konfigurationsoberfläche verschiedene Möglichkeiten zur Verfügung.

Schaltflächen	Beschreibung
Check for Update	Prüft Online auf neue Updates und zeigt eine Release-Information an.
Fetch Update	Lädt ein vorhandenes Update herunter und installiert es automatisch.
Prefetch (reboot manually)	Lädt ein vorhandenes Update herunter, installiert es aber nicht. Die Installation erfolgt erst nach dem nächsten Reboot.

Schaltfläche »Check for Update«

Klicken Sie auf die Schaltfläche »Check for Update«, um Online nach verfügbaren Softwareupdates für SEPPmail zu suchen. Falls ein Update zur Verfügung steht, wird Ihnen dies angezeigt. Zusätzlich wird ebenfalls eine Release-Information angezeigt.

Schaltfläche »Fetch Update«

Zum Installieren eines vorhandenen Updates klicken Sie auf die Schaltfläche »Fetch Update«. Dieser Vorgang kann zeitaufwändig sein, wenn das gelieferte System noch eine ältere Firmware enthält und deshalb mehrere Updates durchgeführt werden müssen. Nach jedem Update erfolgt ein Reboot des Systems.

Wiederholen Sie diesen Schritt, bis keine verfügbaren Updates mehr angezeigt werden. Das System optimiert diesen Update-Prozess, so dass nicht für jede Zwischenversion ein Update installiert werden muss, sondern nur für die Updates, welche die Datenstruktur verändern.

Schaltfläche »Prefetch (reboot manually)«

Für Kunden mit einer Netzwerkinfrastruktur in der Updates nur innerhalb dafür vorgesehener Zeiträume durchgeführt werden können (Wartungsfenster), kann ein Softwareupdate vorab heruntergeladen werden. Das eigentliche Update können Sie im Wartungszeitraum durch Neustarten des SEPPmail-Systems durchführen.

Über die Schaltfläche »Prefetch (reboot manually)« starten Sie den Download des Updates. Nach erfolgtem Download wird eine Statusmeldung unterhalb der Schaltflächen angezeigt. Nach einen Reboot wird das zuvor heruntergeladene Update automatisch installiert.

Allgemeine Hinweise

Es kann unter Umständen vorkommen, dass Sie längere Zeit keine Rückmeldung erhalten. Wenn dies der Fall ist, aktualisieren Sie die Ansicht, indem Sie auf den Link »System Administration« oberhalb der Schaltflächen klicken. Solange Sie nicht ausgeloggt wurden, ist das Update noch nicht abgeschlossen.

Die SEPPmail Appliance muss nach Updates jeweils einen Neustart durchführen und Sie müssen sich neu anmelden. Führen Sie diesen Schritt gegebenenfalls selbst durch, falls das System lange keine Rückmeldung gibt, Ihnen also nicht die Loginmaske angezeigt wird. Prüfen Sie nach dem Neustart erneut, ob weitere Updates zur Verfügung stehen.

Wenn Sie die Meldung »You already have the latest version installed« erhalten, ist Ihre SEPPmail-Appliance auf dem neusten Softwarestand. Sollten in Zukunft weitere Updates verfügbar sein, wird dies nach einem Neustart automatisch im Menü »Home« und im Menü »Administration« angezeigt.

Wenn Sie auf das Menü »Administration« zugreifen wollen und dieser Vorgang dauert sehr lange bzw. länger als gewohnt, dann kann SEPPmail unter Umständen keine Onlineprüfung auf neue Updates durchführen. Prüfen Sie ggf. Ihre Firewallkonfiguration. Das Menü »Administration« wird dann nach etwas längerer Wartezeit trotzdem angezeigt.

6.9.4 Einstellungen der Appliance sichern und wiederherstellen

Menü »Administration« -> Sektion »Backup«

Um die Einstellungen der SEPPmail-Appliance zu sichern oder wiederherzustellen, stehen in der Konfigurationsoberfläche verschiedene Möglichkeiten zur Verfügung.

Wichtiger Hinweis:

Ein Systembackup enthält alle Konfigurationsdaten bis auf die Folgenden:

1. das lokale SSL-Device-Zertifikat
2. das lokale Root-CA-Zertifikat
3. der lokale Cluster-Identifier

Stellen Sie sicher, dass die genannten Ausnahmen vom Systembackup separat manuell gesichert werden. Im Fehlerfall können Sie nur die Daten wiederherstellen die im Systembackup enthalten sind und die Sie zusätzlich zum Systembackup manuell gesichert haben.

Die folgenden Bewegungsdaten sind ebenfalls nicht im Systembackup enthalten:

1. die lokalen Log-Dateien
2. die lokalen System-Statistiken
3. der lokale LFM-Store
4. die lokale E-Mail-Queue

Schaltflächen	Beschreibung
Backup: Download	Manuelles Herunterladen eines Systembackups
Backup: Change Password	Ändern des Backup-Kennworts
Restore: Import Backup File...	Manuelles Zurücksichern eines Systembackups
Restore: Import ldif...	Manuelles Zurücksichern einer LDIF-Datei

Allgemeiner Hinweis zum Backup

Um den aktuellen Stand Ihrer SEPPmail-Appliance zu sichern, müssen Sie zuerst ein Backup-Kennwort festlegen. Dieses wird beim Zurückspielen eines Backups benötigt.

Schaltfäche »Download«

Um die Datensicherung durchzuführen, klicken Sie auf die Schaltfläche »Download«. Sie erhalten eine verschlüsselte Datei zum lokalen Speichern. Für die Verschlüsselung wird das angegebene Kennwort verwendet.

Schaltfäche »Change Password«

Bevor Sie das Erste Backup erstellen ist er erforderlich, dass Sie ein Kennwort zur Sicherung der Backupdateien vergeben. Dieses Kennwort benötigen Sie, um die Backupdatei im Fehlerfall wieder einspielen zu können. Um das Kennwort für zukünftige Backups zu ändern, klicken Sie auf die Schaltfläche »Change Password«.

Achtung, die Änderung wirkt sich nur auf zukünftige Backups aus! Backup-Dateien aus der Vergangenheit sind weiterhin mit dem entsprechenden in der Vergangenheit gesetzten Passwort geschützt.

Schaltfläche »Import Backup File«

Um eine Backup-Datei einzuspielen und somit Einstellungen der Appliance wiederherzustellen, klicken Sie auf die Schaltfläche »Import Backup File...«. Um die Wiederherstellung durchzuführen, wählen Sie im anschliessenden Dialog die Backup-Datei aus und geben Sie das dazugehörige Passwort ein.

6.9.5 Appliance neu starten oder herunterfahren

Menü »Administration« -> Sektion »System«

Schaltfläche	Beschreibung
Reboot...	Neustart des Systems

Schaltfläche	Beschreibung
Shut down...	Herunterfahren des Systems und ausschalten

Um einen ungewollten Neustart oder ein ungewolltes Herunterfahren zu verhindern, müssen diese Vorgänge mit einem Sicherheitscode bestätigt werden. Der Sicherheitscode wird jeweils automatisch generiert und angezeigt und muss von im Feld »Security code« eingegeben werden.

```
Beispiel:

Please enter the security code ivahkagh in the field below.

Hierbei ist die Zeichenfolge »ivahkagh« der Security Code.
```

Dieser muss im Feld »Security code« eingegeben werden. Klicken Sie dann auf die Schaltfläche »Reboot system now...«, um einen Neustart auszuführen. Bei einem Herunterfahren des Systems verfahren Sie analog.

6.9.6 Appliance auf Werkseinstellungen zurücksetzen

Menü »Administration« -> Sektion »Database and System Settings«

Zum Zurücksetzen des Systems auf die Werkseinstellungen klicken Sie auf die Schaltfläche »Perform factory reset...«. Um ein ungewolltes Zurücksetzen des Systems zu verhindern, muss dieser Vorgang mit einem Sicherheitscode bestätigt werden. Der Sicherheitscode wird jeweils automatisch generiert und angezeigt und muss von Ihnen im Feld »Security code« in umgekehrter Reihenfolge (von hinten nach vorne) eingegeben werden.

Nach korrekter Eingabe des Sicherheitscodes und einem Klick auf die Schaltfläche »Factory reset!« erscheint die Bestätigungsmeldung »Factory reset in progress. The device will automatically switch off after finishing«. Sobald der Vorgang abgeschlossen ist, schaltet sich SEPPmail automatisch aus.

Damit alle auf dem System gespeicherten Daten sicher gelöscht werden haben Sie die Möglichkeit, durch das Aktivieren des Parameters »Secure Overwrite (Partitions will be overwritten ten times with random data, might take very long)« die Bereiche des Datenspeichers 10 Mal mit zufälligen Daten zu überschreiben. Dieser Vorgang dauert sehr lange, bietet aber eine höhere Sicherheit vor unberechtigtem Wiederherstellen von gelöschten Daten.

6.9.7 Bestehende Benutzer oder Schlüssel importieren

Menü »Administration« -> Sektion »Import«

Schaltfläche	Beschreibung
Import Users (CSV)	Importieren von Benutzern aus einer CSV-Datei
Import GINA Users (CSV)	Importieren von GINA-Benutzern aus einer CSV-Datei

Schaltfläche	Beschreibung
Import openPGP secret keys	Importieren von OpenPGP Schlüsseln
Import S/MIME keys	Import von S/MIME Schlüsselpaaren
Import S/MIME certificates	Import von S/MIME public-Keys

Schaltfläche »Import Users (CSV): Import«

Benutzerkonten importieren Sie, indem Sie auf die Schaltfläche »Import«, neben »Import Users (CSV)«, klicken. Die Datei mit Benutzerinformationen muss im CSV (Comma-Separated Values) Format vorliegen und folgende Syntax aufweisen: USERID;NAME;EMAIL;PASSWORD. Das Feld »PASSWORD« ist optional. Die importierten Benutzer werden im Menü »Users« angezeigt.

Schaltfläche »Import GINA Users (CSV): Import«

Um GINA-Benutzer zu importieren, klicken Sie auf die Schaltfläche »Import«, neben »Import GINA Users (CSV)«. Die Datei Datei mit Benutzerinformationen muss im CSV-Format vorliegen und folgende Syntax aufweisen: EMAIL;PASSWORD. Die importierten Benutzer werden im Menü »GINA-accounts« angezeigt.

Schaltfläche »Import openPGP secret keys«

Bestehende openPGP-Schlüsselpaare können Sie mit einem Klick auf die Schaltfläche »Import openPGP secret keys« einlesen. Sie können die Schlüssel als Datei oder in Textform importieren. Zusätzlich müssen Sie den Passphrase des jeweiligen Schlüssels eingeben. Wenn Sie eine größere Menge von OpenPGP Keys auf einmal importieren wollen, müssen diese Schlüssel in einer Schlüsseldatei zusammengefasst vorliegen. Beim Import der OpenPGP Schlüsselpaare wird für jedes Schlüsselpaar ein Benutzerkonto angelegt. Jedem Benutzerkonto wird das passende OpenPGP Schlüsselpaar automatisch zugeordnet.

Schaltfläche »Import S/MIME keys«

Bestehende S/MIME-Zertifikate (Schlüsselpaare) können Sie mit einem Klick auf die Schaltfläche »Import S/MIME keys« einlesen. Die Zertifikate müssen als Datei im Format PKCS#12 vorliegen. Um eine größere Menge von S/MIME Zertifikaten auf einmal zu importieren (Bulk), können Sie diese in einem ZIP-Archiv zusammenfassen. Dieses ZIP-Archiv darf keine Verzeichnisstruktur enthalten und nicht durch ein Kennwort gesichert sein. Beim Import der S/MIME-Zertifikate (Schlüsselpaare) wird für jedes Schlüsselpaar ein Benutzerkonto angelegt. Jedem Benutzerkonto wird das passende S/MIME Schlüsselpaar automatisch zugeordnet.

Schaltfläche »Import S/MIME certificates«

Bestehende S/MIME-Public Keys können Sie mit dem Klick auf die Schaltfläche »Import S/MIME certificates« einlesen. Die eingelesenen Zertifikate werden im SEPPmail eigenen Zertifikatsspeicher abgelegt. Die eingelesenen S/MIME-Public Keys finden Sie im Menü »X.509 Certificates«

6.9.8 Ausgehende Supportverbindung herstellen

Menü »Administration« -> Sektion »Establish Support Connection«

Mit der Schaltfläche »Establish Support Connection« wird eine Verbindung zum Hersteller geöffnet. Verwenden Sie diese Funktion nur auf Anweisung des Herstellers. Damit die Verbindung aufgebaut werden kann, muss auf Ihrer Firewall bzw. Ihrem Router Port TCP/22 (SSH) von der SEPPmail Appliance ins Internet geöffnet sein.

Um eine eingehende Supportverbindung herzustellen, klicken Sie in der Konfigurationsoberfläche auf den Menüpunkt »Administration« und anschließend auf die Schaltfläche »Connect«.

6.10 Menüpunkt "Cluster"

Dieses Kapitel beschreibt die grundsätzliche Funktionsweise und die Verwaltung des SEPPmail-Cluster. Sie erfahren, welche Cluster Betriebsarten durch SEPPmail unterstützt werden und wie Sie diese in der Konfigurationsoberfläche einrichten können.

6.10.1 Allgemein

Es gibt verschiedene Arten eines Cluster-Betriebs die durch SEPPmail unterstützt werden.

Ein Cluster bezeichnet einen Rechnerverbund aus mehreren vernetzten Computersystemen. Diese miteinander vernetzten Computersysteme sind zwar physisch getrennt werden aber logisch als eine Einheit betrachtet. So ist es möglich, dass ein Cluster als ein einziges logisches System angesprochen werden kann, tatsächlich aber aus mehreren physischen Systemen besteht.

Für den Einsatz eines Clusters gibt es verschiedene Zielsetzungen die sich ja nach Anwendung unterscheiden. Für ein Cluster aus mehreren SEPPmail Systemen gibt es die folgenden 4 Betriebsarten:

1. Hochverfügbarkeitscluster zur Ausfallsicherheit (Failover)
2. Load Balancing Cluster zur Lastverteilung
   - Aufteilung des eingehenden und ausgehenden Mailflusses auf je ein Cluster Member System
   - Einsatz eines externen Load Balancers, zum verteilen des E-Mails auf verschiedene Cluster Member Systeme (je nach Konfiguration)
   - Lastverteilung basierend auf dem DNS Round Robin Verfahren (http://de.wikipedia.org/wiki/Lastverteilung_per_DNS)
3. Geo Cluster zum replizieren von Konfigurationsdatenbanken auf geografisch voneinander entfernte Systeme
4. Frontend-Backend Cluster

In den folgenden Abschnitten sind die jeweiligen 4 Betriebsarten im Detail beschrieben.

6.10.2 Hochverfügbarkeitscluster

Die Ausfallsicherheit des SEPPmail Systems kann durch die Bildung eines Clusters erhöht werden.

Das SEPPmail System besitzt eine integrierte Clusterfunktionalität auf Basis des CARP Protokolls (http://de.wikipedia.org/wiki/Common_Address_Redundancy_Protocol).

Um einen Cluster zu bilden sind mindestens zwei SEPPmail Systeme erforderlich die sich gegenseitig überwachen. Fällt ein System aus bzw. antwortet dieses nicht mehr auf Überwachungsanfragen, so übernimmt das zweite System dessen Funktion. Ist das ausgefallene System wieder verfügbar bzw. es

antwortet wieder auf Überwachungsanfragen, so übernimmt es wieder seine ursprüngliche Aufgabe.

Diese Funktion kann mit bis zu 9 SEPPmail Systemen abgebildet werden, wodurch Sie eine sehr hohe Ausfallsicherheit erreichen können.

Das Hochverfügbarkeitscluster kann mit SEPPmail Systemen auf Hardwarebasis und auf Basis der Virtualisierung mit VMware ESX abgebildet werden. Ein Mischbetrieb mit Systemen auf Hardwarebasis und virtualisierten Systemen ist ebenfalls möglich.

Wie funktioniert das Hochverfügbarkeitscluster?

Bei diesem Verfahren werden einem Cluster eine oder mehrere virtuelle IP Adresse(n) mit verschiedenen Prioritäten zugeordnet. Jedes Cluster Member System hat unabhängig von der zugewiesenen virtuellen Cluster IP-Adresse eine jeweils eigene eindeutige IP-Adresse. Über diese eigene eindeutige IP-Adresse kann jedes Cluster Member System explizit angesprochen werden.

Beispiel:
In der folgenden Abbildung ist die virtuelle Cluster IP-Adresse des Clusters 10.10.0.1. Die Cluster Member Systeme haben in unserem Beispiel die IP Adressen 10.10.0.9 und 10.10.0.10.

Abbildung 1 - Schematische Darstellung eines Hochverfügbarkeitsclusters

Das Cluster selbst wird von anderen Systemen, z.B. einem internen E-Mail Server oder einem vorgelagerten E-Mail Relay Server (Gateway) über die eingerichtete(n) virtuelle(n) IP-Adresse(n) angesprochen. Im Beispiel oben ist das die IP-Adresse 10.10.0.1.

Wird das Cluster selbst über seine Cluster IP-Adresse angesprochen, so reagiert immer das Cluster Member System mit der höchsten Priorität auf die angesprochene virtuelle Cluster IP-Adresse. Alle anderen Cluster Member Systeme mit niedrigerer Priorität reagieren nicht, wenn die virtuelle Cluster IP-Adresse angesprochen wird und ein Cluster Member System mit einer höheren Priorität verfügbar ist.

Im Fehlerfall, falls ein Cluster Member System mit höherer Priorität ausfällt, welches normalerweise auf die angesprochene virtuelle Cluster IP-Adresse reagiert, so übernimmt automatisch ein Cluster Member System mit der nächst niedrigeren Priorität die virtuelle Cluster IP Adresse inclusive der Funktion des ausgefallenen Cluster Member Systems.

Die Prioritäten sind in der folgenden Reihenfolge geordnet:

1. Primary
2. Secondary
3. Backup

Das Einrichten der Priorität des jeweiligen Cluster Member Systems führen Sie im Menü »System« durch.

6.10.3 Load Balancing Cluster

Ein Cluster kann zusätzlich zur Erhöhung des E-Mail Durchsatzes verwendet werden. Hierfür gibt es die folgenden Möglichkeiten:

1. Aufteilung des eingehenden und ausgehenden E-Mail Datenflusses auf je ein Cluster Member System 125
2. Einsatz eines externen Load Balancers, zum Verteilen der E-Mails auf verschiedene Cluster Member Systeme (je nach Konfiguration) 127
3. Lastverteilung basierend auf dem DNS Round-Robin-Verfahren 128 (http://de.wikipedia.org/wiki/Lastverteilung_per_DNS)

Einsatz mit redundanten externen und internen MTAs (Mail Transport Agent) 130

Das Failover-Verhalten des Clusters wird durch diese Konfigurationen nicht verändert.

Aufteilung des eingehenden und ausgehenden E-Mail Datenflusses auf je ein Cluster Member System

Die Aufteilung des ein- und ausgehenden E-Mail Datenflusses kann, wie bereits erwähnt, auf drei verschiedene Arten erfolgen. In Abbildung 1 werden ein- und ausgehende E-Mails durch eine statische Konfiguration jeweils an eine separate virtuelle IP-Adresse gesendet. Es existieren 2 SEPPmail Systeme die mit unerschiedlicher Priorität auf jeweils zwei virtuelle IP-Adressen (Alias IP-Adressen) reagieren. Jeweils ein System erhält alle eingehenden E-Mails und ein System erhält alle ausgehenden E-Mails. Durch das Einrichten von zwei virtuellen IP-Adressen können die beiden SEPPmail Systeme über eine dedizierte virtuelle IP-Adresse separat angesprochen werden.

In Abbildung 1 ist dies logisch abgebildet. Physisch existieren lediglich zwei SEPPmail Systeme.

Was passiert im Detail:

Jedes SEPPmail System hat eine eigene völlig separate IP-Adresse über die nur dieses System angesprochen werden kann, z.B. für die Konfiguration von Einstellungen die nicht im Cluster synchronisiert werden.

In Abbildung 1 sind dies die IP-Adressen 10.10.0.9 und 10.10.0.10.

Zusätzlich gibt es zwei virtuelle IP-Adressen, um die beiden SEPPmail Systeme logisch zu jeweils einer Gruppe zusammenzufassen. In Abbildung 1 sind diese virtuellen IP-Adressen (Gruppen) farblich getrennt dargestellt.

Die virtuelle IP-Adresse 10.10.0.1, hier grün dargestellt, wird für alle ausgehenden E-Mails vom internen E-Mail Server angesprochen bzw. die ausgehenden E-Mails werden vom internen E-Mail Server an diese virtuelle IP-Adresse gesendet.

Die virtuelle IP-Adresse 10.10.0.2, hier orange dargestellt, wird für alle eingehenden E-Mails vom externen E-Mail Server oder auch einem vorgelagerten E-Mail Relay (z.B. Firewall) angesprochen bzw. die eingehenden E-Mails werden von den externen oder vorgelagerten Systemen an diese virtuelle IP-Adresse gesendet.

Unter einer virtuellen IP-Adresse sind nun die beiden physichen SEPPmail Systeme logisch zusammengefaßt. Grundsätzlich reagieren beide Systeme, wenn die virtuelle IP-Adresse

angesprochen wird. Dies ist aber nicht immer sinnvoll, da wir jeweils ein System für alle eingehenden E-Mails verwenden wollen und das andere System für alle ausgehenden E-Mails. Um dies zu erreichen ist die Reihenfolge in der die einzelnen Systeme antworten sollen in einer Hierarchie festgelegt, wenn eine der beiden virtuellen IP-Adressen angesprochen wird.

In Abbildung 1, grün dargestellt, sehen Sie die virtuelle IP-Adresse 10.10.0.1 für alle ausgehenden E-Mails. Hier ist das Cluster Member System mit der IP-Adresse 10.10.0.9 als Primary eingerichtet und reagiert immer als erstes System, wenn die virtuelle IP-Adresse 10.10.0.1 angesprochen wird. Das Cluster Member System mit der IP-Adresse 10.10.0.10 ist als Secondary eingerichtet und reagiert nur dann, wenn der Cluster Member Primary nicht verfügbar ist.

In Abbildung 1, orange dargestellt, sehen Sie die virtuelle IP-Adresse 10.10.0.2 für alle eingehenden E-Mails. Hier ist das Cluster Member System mit der IP-Adresse 10.10.0.10 als Primary eingerichtet (entgegengesetzt der vorherigen Darstellung) und reagiert immer als erstes System, wenn die virtuelle IP-Adresse 10.10.0.2 angesprochen wird. Das Cluster Member System mit der IP-Adresse 10.10.0.9 ist als Secondary eingerichtet und reagiert nur dann, wenn der Cluster Member Primary nicht verfügbar ist.

Zusammenfassung:

Jedes einzelne SEPPmail System kann über zwei verschiedene virtuelle IP-Adressen angesprochen werden und reagiert mit jeweils unterschiedlichen Prioritäten einmal als Primary und einmal als Secondary. Dadurch ist der Betrieb beim Ausfall eines Cluster Member Systems weiterhin möglich. Das verbliebene Cluster Member System übernimmt dann die Arbeit des nicht mehr verfügbaren Systems und wird alle ein- und ausgehenden E-Mails verarbeiten.

Für die Nutzung von Enhanced Secure Webmail kann eine virtuelle Cluster IP-Adresse 10.10.0.1 angesprochen werden. In Abhängigkeit der Cluster Member Prioritäten wird im Beispiel in Abbildung 1 das Cluster Member System mit der IP-Adresse 10.10.0.9 antworten, da dies mit der Priorität »Primary« eingerichtet ist. Ist dieses System nicht verfügbar, so wird das Cluster Member System mit der IP-Adresse 10.10.0.10 antworten, da dies mit der Priorität »Secondary« eingerichtet ist.

Das einrichten der virtuellen IP-Adressen und das Zuweisen den Prioritäten führen Sie im Menü »System« durch.

Abbildung 1 - Schematische Darstellung der statischen Aufteilung für ein- und ausgehenden E-Mails

Einsatz eines externen Load Balancers, zum Verteilen der E-Mails auf verschiedene Cluster Member Systeme
In Abbildung 2 werden ein- und ausgehende E-Mails durch einen externen Load Balancer dynamisch an die Cluster Member Systeme gesendet. Jedes Cluster Member System erhält dadurch gleichermaßen ein- und ausgehende E-Mails. Falls ein Cluster Member System nicht mehr verfügbar ist, so ist der Load Balancer dafür verantwortich dies zu erkennen und entsprechend zu reagieren. Abbildung 2 zeigt eine logische Darstellung des Szenarios.

Was passiert im Detail:

Die Clusterfunktionalität von SEPPmail wird in diesem Szenario lediglich für die Synchronisation der Konfiguration zwischen den Cluster Member Systemen verwendet. Die Entscheidung, welches System auf ein- und ausgehende E-Mails reagiert wird durch den vorgelagerten Load Balancer getroffen. Dieser verteilt je nach Konfiguration und Lastsituation die E-Mails an wahlweise an ein Cluster Member System. Hierbei wird das Cluster Member System nicht über eine virtuelle IP-Adresse angesprochen sondern über seine eigene separate IP-Adresse.

Jedes SEPPmail System hat eine eigene völlig separate IP-Adresse über die nur dieses System angesprochen werden kann, z.B. für die Konfiguration von Einstellungen die nicht im Cluster synchronisiert werden.

In Abbildung 2 sind dies die IP-Adressen 10.10.0.9 und 10.10.0.10.

Der wesentliche Unterschied zur Abbildung 1 ist, dass hierbei keine virtuelle IP-Adresse angesprochen wird. Zum Verteilen ausgehender E-Mails wird der Load Balancer am internen E-Mail Server diese wahlweise an die Cluster Member Systeme mit den IP-Adressen 10.10.0.9 und 10.10.0.10 verteilen.

Zusammenfassung:

Beim Einsatz eines externen Load Balancers werden die SEPPmail Cluster Member Systeme direkt vom Load Balancer angesprochen. Falls ein Cluster Member System ausfällt, so ist der Load Balancer dafür verantwortlich dies zu erkennen und die ein- oder ausgehenden E-Mails an das verbleibende System zu senden.

Für die Nutzung von Enhanced Secure Webmail kann weiterhin die virtuelle Cluster IP-Adresse angesprochen werden. In Abhängigkeit der Cluster Member Prioritäten wird im Beispiel in Abbildung 2 das Cluster Member System mit der IP-Adresse 10.10.0.9 antworten, da dies mit der Priorität »Primary« eingerichtet ist. Ist dieses System nicht verfügbar, so wird das Cluster Member System mit der IP-Adresse 10.10.0.10 antworten, da dies mit der Priorität »Secondary« eingerichtet ist.

Das einrichten der virtuellen IP-Adressen und das Zuweisen den Prioritäten führen Sie im Menü »System« durch.

Abbildung 2 - Schematische Darstellung der dynamischen Aufteilung für ein- und ausgehende E-Mails durch einen externen Load Balancer

Lastverteilung basierend auf dem DNS Round-Robin-Verfahren

Eine detailierte Beschreibung dieser Funktion finden Sie im folgenden Artikel: http://de.wikipedia.org/wiki/Lastverteilung_per_DNS

In der Konfiguration des internen und externen E-Mail Servers wird nicht mehr eine virtuelle Cluster IP-Adresse für den E-Mail Versand angegeben sondern jeweils ein Hostname, z.B. »cluster-in.domain.tld« oder »cluster-out.domain.tld«, der bei ein- und ausgehenden E-Mails angesprochen wird. Im DNS ist es möglich zu jedem Hostnamen mehrere IP-Adressen anzugeben. Dadurch kann eine einfache Lastverteilung erreicht werden.

Fragt z.B. der internen E-Mail Server den für den E-Mail Versand angegebenen Hostnamen des SEPPmail Clusters beim DNS an, so werden immer alle diesem Hostnamen zugeordneten IP-Adressen zurückgeliefert, dies aber jedes Mal in unterschiedlicher Reihenfolge. Der interne E-Mail Server kann nun eine dieser IP-Adressen zum Versand der E-Mail auswählen. Im Fehlerfall wird das im Cluster mit der nächst niedrigeren Priorität verfügbare Cluster Member System antworten. Abbildung 3 zeigt eine logische Darstellung des Szenarios.

Was passiert im Detail:

Jedes SEPPmail System hat eine eigene völlig separate IP-Adresse über die nur dieses System angesprochen werden kann, z.B. für die Konfiguration von Einstellungen die nicht im Cluster synchronisiert werden.

In Abbildung 3 sind dies die IP-Adressen 10.10.0.9 und 10.10.0.10.

Zusätzlich gibt es zwei virtuelle IP-Adressen, um die beiden SEPPmail Systeme logisch zu jeweils einer Gruppe zusammenzufassen. In Abbildung 3 sind diese virtuellen IP-Adressen (Gruppen) farblich getrennt dargestellt.

Der interne und der externe E-Mail Server sprechen für den Versand von ein- und ausgehenden E-Mails an das SEPPmail Cluster System einen Hostnamen statt einer virtuellen IP-Adresse an. Wird eine Anfrage für diesen Hostnamen an den DNS-Server gestellt, so wird der Hostname in alle

eingerichteten IP-Adressen aufgelöst.

In unserem Fall entsprechenden die aufgelösten IP-Adressen den virtuellen Cluster IP-Adressen wie in Abbildung 3 dargestellt. Die beiden virtuellen IP-Adressen haben jeweils ein anderes System als Cluster Member Primary und Cluster Member Secondary. Hierdurch ist eine Redundanz im Fehlerfall gegeben, da sich beide Cluster Member Systeme überwachen und jeweils die Aufgabe des ausgefallenen Systems übernehmen können.

Die virtuelle IP-Adresse 10.10.0.1, hier grün dargestellt, und die virtuelle IP-Adresse 10.10.0.2, hier orange dargestellt, werden dem Hostnamen zugeordnet, der z.B. im internen E-Mail Server für den Versand von ausgehende E-Mails eingetragen ist. Dieser Hostname wird in die folgenden IP-Adressen aufgelöst:

custer-out.domain.tld. 1800 IN A 10.10.0.1
custer-out.domain.tld. 1800 IN A 10.10.0.2

Bei jeder Auflösung des angesprochenen Hostnamen »cluster-out.domain.tld« wird der DNS Server alle zugeordneten IP-Adressen zurückliefern, allerdings in anderer Reihendolge.

custer-out.domain.tld. 1800 IN A 10.10.0.2
custer-out.domain.tld. 1800 IN A 10.10.0.1

Der interne E-Mail Server kann nun eine IP-Adresse auswählen und die ausgehende E-Mail versenden. Da sich bei jeder Anfrage die Reihenfolge der zurückgelieferten IP-Adressen ändern, können die E-Mails auf die zur Verfügung stehenden Cluster Member Systeme verteilt werden.

Zusammenfassung:

Beim Versand von ein- und ausgehenden E-Mails über das SEPPmail Cluster wird statt einer virtuellen Cluster IP-Adresse ein Hostname im jeweiligen E-Mail Server angegeben. Dieser wird dann zur Laufzeit in die zugehörigen IP-Adressen aufgelöst. So können der interne und der externe E-Mail Server ein- und ausgehende E-Mails wahlweise an eine dieser aufgelösten IP-Adressen senden. Da es sich hierbei jeweils um virtuelle Cluster IP-Adressen handelt reagieren die Cluster Member Systeme je nach Priorität, z.B. im Fehlerfall.

Durch die DNS Round-Robin-Funktion kann für den ein- und ausgehenden E-Maildatenfluss eine Lastverteilung erreicht werden.

Quelle: Wikipedia, http://de.wikipedia.org/wiki/Lastverteilung_per_DNS (auch auszugsweise in diesem Kapitel wiedergegeben)

Das einrichten der virtuellen IP-Adressen und das Zuweisen den Prioritäten führen Sie im Menü »System« durch.

Abbildung 3 - Schematische Darstellung der Lastverteilung durch das DNS Round-Robin-Verfahren für ein- und ausgehende E-Mails

Einsatz mit redundanten internen und externen MTAs (Mail Transport Agent)

In der SEPPmail Konfiguration kann als externer MTA (E-Mail Relay) genau 1 Host konfiguriert werden. Analog kann pro interner E-Mail Domain genau 1 interner MTA (E-Mail Server) konfiguriert werden. Das SEPPmail System kann redundante externe und interne MTAs mit dem in den folgenden Abschnitten erläuterten Verfahren unterstützen.

Im SEPPmail System kann der externe bzw. der interne MTA auf mehrere Arten konfiguriert werden:

- Angabe einer IP Adresse
- Angabe eines Hostnamens
- Angabe einer Domain, für die ein MX Lookup durchgeführt wird

Die Unterscheidung zwischen IP Adresse, Hostname und Domain erfolgt mittels eckiger Klammern (»[« , »]«): IP Adressen und Hostnamen müssen in eckigen Klammern angegeben werden, Domains, für die ein MX Lookup durchgeführt wird, ohne eckige Klammern.

Das SEPPmail System kann redundante externe oder interne MTAs unterstützen, indem für den externen und den internen MTA je eine nur intern verfügbare Dummy-Domain konfiguriert wird. Für jede Dummy-Domain werden 2 MX Records mit unterschiedlichen Preferences im internen DNS angelegt. Das SEPPmail System leitet E-Mails standardmässig an den Host mit der niedrigsten Preference weiter. Beim Ausfall dieses Hosts werden E-Mails automatisch an den Host mit der höheren Preference geleitet.

Das einrichten der Hostnamen für die redundanten internen und externen MTAs führen Sie im Menü »Mail System« durch.

Load Balancing Cluster - redundante interne und externe MTAs

redundante interne
E-Mail Server

Cluster Member Primary
IP:10.10.0.9

vollautomatische
Synchronisierung

Cluster Member Secondary
IP:10.10.0.10

virtuelle Cluster
IP-Adresse: 10.10.0.1

redundante externe
E-Mail Server

Abbildung 4 - Schematische Darstellung für den Einsatz von redundanten internen und externen MTAs

6.10.4 Geo Cluster

Ein Geo-Cluster (auch »Multisite System« genannt) dient zum replizieren von Konfigurationsdatenbanken zwischen geografisch voneinander entfernten SEPPmail Systemen an verschiedenen Standorten des Unternehmens.

Einsatzbeispiel:

Ein Unternehmen ist weltweit tätig und betreibt aus diesem Grund mehrere Datacenter auf verschiedenen Kontinenten. Die Unternehmensstandorte selbst sind alle durch ein VPN verbunden und haben in jedem Datacenter einen Zugang zum Internet. Innerhalb dieses internen Unternehmensnetzwerks besteht ein E-Mail Transportsystem, z.B. auf Basis von Microsoft Exchange oder Lotus Notes. Die nach extern gesendeten E-Mails können je nach intern abgebildeter Richtlinie an verschiedenen Internetzugängen des Unternehmens ins Internet versendet werden. (z.B. falls ein Internetzugang an einem Standort nicht funktioniert, die VPN-Verbindung zwischen den Standorten davon aber nicht betroffen ist und dadurch der externe Versand von E-Mails nun über einen anderen Standort durchgeführt wird)

Dazu ist es erforderlich, dass die notwendige kryptografische E-Mail Verarbeitung an allen Internetzugängen gleich erfolgt. Es müssen alle Benutzerkonten und deren Zertifikate zu Signieren, Entschlüsseln und Verschlüsseln vorhanden sein und auch die Konfigurationseinstellungen müssen identisch sein um keine Abweichungen bei der E-Mail Verabeitung zu haben.

Durch die Geo-Cluster Funktion des SEPPmail Systems können Konfigurationsänderungen zwischen allen SEPPmail Systeme im Geo-Cluster sofort repliziert werden. Somit ist eine konsistente Konfiguration alle Systeme gewährleistet.

Geo Cluster - MultiSite System
@ Internet
ein- und ausgehende E-Mails
Firmennetzwerk Datacenter Standort A
Firmennetzwerk Datacenter Standort B
interner E-Mail Server
Cluster Member Primary IP-Adresse:10.10.0.2
vollautomatische Synchronisierung
Cluster Member Secondary IP-Adresse:10.10.0.3
Cluster Synchronisierung durch VPN-Tunnel
Cluster Member Primary IP-Adresse:20.20.0.2
vollautomatische Synchronisierung
Cluster Member Secondary IP-Adresse:20.20.0.3
interner E-Mail Server
virtuelle Cluster IP-Adresse: 10.10.0.1
virtuelle Cluster IP-Adresse: 20.20.0.1
firmeninternes E-Mail Transportnetzwerk via VPN-Tunnel

Abbildung 1 - Schematische Darstellung einer Geo-Cluster Struktur

6.10.5 Frontend-Backend Cluster

Frontend-Backend Cluster, wobei die Frontend Systeme keine lokale Konfigurationsdatenbank besitzen

Das Betreiben eines SEPPmail Systems als Frontend Server ist eine sehr spezielle Cluster Funktion. Der Unterschied zur normalen Cluster Funktion des SEPPmail Systems besteht darin, dass auf dem Frontend Server selbst keine Konfigurationsdatenbank existiert.

Die zur Laufzeit benötigten Konfigurationsdaten werden ja nach Anforderung, z.B. beim notwendigen Entschlüsseln einer eingehenden E-Mail, vom Cluster auf den Frontend Server transferiert und nur temporär vorgehalten. Nach der E-Mail Verarbeitung werden diese Konfigurationsdaten sofort wieder gelöscht.

Diese Funktion kann in Szenarien Anwendung finden die entsprechende Anforderungen an die Compliance stellen.

Abbildung 1 - Schematische Darstellung einer Frontend-Backend Cluster Struktur

6.10.6 Einrichten einer Clusterkonfiguration

Wichtiger Hinweis:

Bitte beachten Sie die Sicherheitshinweise, wenn Sie Änderungen an den Parametern des Clusterverbunds vornehmen, Systeme aus dem Clusterverbund herauslösen, Systeme im Fehlerfall ersetzten oder neue Systeme dem Clusterverbund hinzufügen.

Ohne das Beachten dieser Sicherheitshinweise können Sie den kompletten Clusterverbund unbrauchbar machen.

Die Sicherheitshinweise finden Sie im Kapitel Sicherheitshinweise 137.

Sektion	Parameter	Beschreibung
Prepare for Cluster	use this key to add a different device to this device/cluster	Schaltfläche »Download Cluster Identifier« Wählen Sie die Schaltfläche »Download Cluster Identifier«, um den systemeigenen RSA PRIVATE KEY herunterzuladen und als Datei lokal zu speichern. Die heruntergeladene Datei hat den Dateinamen »clusterid.txt«. Eine Cluster-Identifizierung wird benötigt, um eine weitere SEPPmail-Appliance zu diesem Gerät hinzuzufügen und somit einen Cluster-Verbund zu bilden.
Add this device to existing cluster WARNING: All data except network configuration of this device will be lost	Cluster Identifier	Importieren Sie in diesem Eingabefeld die »Cluster Identifier« Datei eines bestehenden SEPPmail-Cluster-Systems. Das lokale System wird dem bereits bestehenden Cluster hinzugefügt. Bitte beachten Sie die Sicherheitshinweise, wenn Sie ein neues System einem bestehenden Clusterverbund hinzufügen. Fahren Sie mit der weiteren Einrichtung des Clusters erst dann fort, wenn Sie das Prinzip der Einrichtung eines Clusterverbunds komplett verstanden haben! Ohne das Beachten der Sicherheitshinweise können Sie den kompletten Clusterverbund unbrauchbar machen. Die Sicherheitshinweise finden Sie im Kapitel Sicherheitshinweise 137.

Sektion	Parameter	Beschreibung
	Cluster Member IP	IP of the device you want to connect to. Do NOT use an IP alias address! Geben Sie hier die eindeutige IP-Adresse eines SEPPmail-Systems ein, welches bereits Bestandteil des Clusters ist zudem Sie dieses System hinzufügen wollen. Verwenden Sie keine virtuelle IP-Adresse des Clusters! Siehe Menü »System > IP-Adresses« in der Konfigurationsoberfläche. Die Verbindung der Cluster Systeme untereinander erfolgt über eine Secure Shell Verbindung auf Port TCP/22. Verändern Sie diese Port Einstellung nicht.
	IP address of this device	IP address other devices in the cluster can use to connect to this device. Do NOT use an IP alias address! Geben Sie hier die eindeutige IP-Adresse des lokalen Systems ein, welches dem bestehenden Cluster hinzugefügt werden soll. Siehe Menü »System > IP-Adresses« in der Konfigurationsoberfläche. Die Verbindung der Cluster Systeme untereinander erfolgt über eine Secure Shell Verbindung auf Port TCP/22. Verändern Sie diese Port Einstellung nicht.
	Connect	Schaltfläche »Start« Wählen Sie die Schaltfläche »Start«, nachdem Sie alle notwendigen Werte für die entsprechenden Parameter eingegeben haben,um die Cluster Funktion auf dem lokalen System zu starten. Dieses System wird nun Bestandteil des Cluster-Verbunds.
Add this device as frontend server (no local database)	Cluster Identifier	Importieren Sie in diesem Eingabefeld die »Cluster Identifier« Datei eines bestehenden SEPPmail-Cluster-Systems. Das lokale System wird dem bereits bestehenden Cluster als spezielle Frontend Server hinzugefügt.
	Existing Appliance IP	IP (or virtual IP) of the device (or cluster) you want to connect to. Geben Sie hier die eindeutige IP-Adresse oder die virtuelle Cluster IP-Adresse eines SEPPmail-

Sektion	Parameter	Beschreibung
		Systems ein, welches bereits Bestandteil des Clusters ist zudem Sie dieses System hinzufügen wollen. Die Verbindung der Cluster-Systeme untereinander erfolgt über eine Secure Shell Verbindung auf Port TCP/22. Verändern Sie diese Port Einstellung nicht.
	Connect	Schaltfläche »Start« Wählen Sie die Schaltfläche »Start«, nachdem Sie alle notwendigen Werte für die entsprechenden Parameter eingegeben haben,um die Cluster Funktion auf dem lokalen System zu starten. Dieses System wird nun Bestandteil des Cluster-Verbunds als Frontend Server.

Referenz der Menü Parameter im Menüpunkt »Cluster«

6.10.6.1 Überblick

Das Vorgehen für die Einrichtung und den Betrieb eines SEPPmail-Clusters wird in diesem Kapitel beschrieben. Das in unserem Konfigurationsbeispiel eingerichtete SEPPmail-Cluster besteht aus zwei Systemen. In den folgenden Abschnitten dieses Kapitels werden alle notwendigen Konfigurationsschritte detailliert beschrieben.

Konfigurationsschritte:

1. Erstes SEPPmail-System vollständig einrichten

2. Zweites SEPPmail-System einrichten

3. Beim zweiten SEPPmail-System werden nur die Einstellungen im Menü »System«, die Registrierung des Systems im Menü »Administration« und der Import des SSL-Device Zertifikats im Menü »SSL« benötigt, alle übrigen Einstellungen wie z.B. die Einstellungen im Menü »Mail Processing« und weitere werden beim Erstellen des Clusters automatisch übernommen.

4. In einer virtualisierten Umgebung muss eine zweite virtual Appliance importiert werden. Diese darf kein Duplikat der bestehenden ersten Instanz sein.

5. Im ersten SEPPmail-System die Cluster Identifizierung herunterladen.

6. Das Zweite SEPPmail-System dem Cluster hinzufügen.

7. Festlegung und Konfiguration der virtuellen IP Adresse(n) des Clusters. Je nach Betriebsart des Clusters werden eine oder zwei virtuelle IP Adressen benötigt.
   Wird das Cluster als reiner Hochverfügbarkeitscluster (Failover-Cluster) betrieben (keine Aufteilung des ein- und ausgehenden E-Mail-Datenflusses), dann wird nur eine virtuelle Cluster IP-Adresse benötigt.

   Wird das Cluster zusätzlich für Load-Balancing zur Erhöhung der Performance eingerichtet, dann werden zwei virtuelle Cluster IP-Adressen benötigt.

Auch bei dieser Betriebsart, Hochverfügbarkeitscluster mit zusätzlichem Load-Balancing, bleibt das Failover-Verhalten des Clusters erhalten.

6.10.6.2 Sicherheitshinweise

Wenn Sie ein neues SEPPmail-System einem bestehenden Clusterverbund hinzufügen oder erstmalig einen Clusterverbund erzeugen, so wird die gesamte bestehende Clusterkonfiguration auf dieses neue Cluster Member System repliziert und danach ständig mit dem Clusterverbund synchronisiert.

Alle Daten auf diesem System mit Ausnahme der Einstellungen in den Menüs »System« und »SSL« sowie den Log-Dateien und Statistiken in den Menüs »Logs«, »Webmail Logs« und »Statistics« gehen verloren.

Dies ist insofern wichtig, falls sich auf diesem System noch benötigte Daten wie z.B. S/MIME-Zertifikate, PGP-Schlüssel, GINA-Benutzerkonten etc. befinden.

Weiterhin ist es sehr wichtig zu verstehen, in welcher Reihenfolge SEPPmail-Systeme einem bestehenden Clusterverbund hinzugefügt werden müssen bzw. welches System die Replikationsquelle und welches System das Replikationsziel ist. Falls Sie diese Systeme beim erstellen eines neues Clusterverbunds verwechseln so kann es passieren, dass ein bestehendes und eingerichtetes SEPPmail-System mit leeren Daten des neu hinzugefügten Systems überschrieben wird. Noch viel wichtiger ist dies bei einem bestehenden Clusterverbund der bereits aus mehreren Cluster Member Systeme besteht. Das Verwechseln von Replikationsquelle und Replikationsziel bedeutet in diesem Fall, den kompletten Clusterverbund mit leeren Daten des neuen Systems zu überschreiben.

Der gesamte Clusterverbund wäre dann unbrauchbar. Bitte bedenken Sie dies bei der Konfiguration.

6.10.6.3 Konfiguration der VMware ESX Umgebung

Für den Aufbau und Betrieb eines SEPPmail-Clusters auf Basis virtueller Maschinen in einer VMware ESX Umgebung ist es erforderlich, die Sicherheitseinstellungen des vSwitch und den entsprechenden Portgruppen wie folgt einzurichten:

Im VMware vSphere Client wählen Sie »Bestandsliste -> ESX-Server -> [Reiter Konfiguration] -> Netzwerk«

vSwitch0 Eigenschaften

Ports | Netzwerkadapter

Konfiguration	Übersicht
vSwitch	56 Ports
VM Network	Portgruppe der virtuellen Maschine
Service Console	Servicekonsolenport

Portgruppeneigenschaften

Netzwerkbezeichnung: VM Network
VLAN-ID: Keine

Effektive Richtlinien

Sicherheit

Promiscuous-Modus: Akzeptieren
MAC-Adressenänderungen: Akzeptieren
Gefälschte Übertragungen: Akzeptieren

Traffic-Shaping

Durchschnittliche Bandbreite: N/A
Spitzenbandbreite: N/A
Burstgröße: N/A

Failover und Lastausgleich

Lastenausgleich: Port-ID
Netzwerkausfallerkennung: Nur Verbindungsstatus
Switches benachrichten: Ja
Failback: Ja
Aktive Adapter: vmnic0
Standby-Adapter: Keine
Nicht verwendete Adapter: Keine

Hinzufügen... Bearbeiten... Entfernen

Schließen Hilfe

Abbildung 1 - Sicherheitseinstellung der Portgruppen im vSwitch eines VMware ESX Systems

6.10.6.4 Einrichten der Basiseinstellungen eines SEPPmail Systems

Um ein SEPPmail-Cluster-System einzurichten müssen auf den zugehörigen Systemen einige Basiseinstellungen vorgenommen werden. Alle weiteren Einstellungen werden beim Aufbau eines Clusters oder dem Hinzufügen eines neuen SEPPmail-Systems zu einem bestehenden Cluster automatisch auf das neue Cluster Member System repliziert. Danach synchronisieren sich alle Cluster Member Systeme untereinander, wenn auf einem Cluster Member System eine Veränderung der Konfigurationsparameter oder der Bewegungsdaten erfolgt. Die Bewegungsdaten beinhalten PGP und S/MIME Benutzerzertifikate/Domainzertifikate sowie X.509 Root Zertifikate.

Die Basiseinstellungen beinhalten die folgenden statischen systemspezifischen Konfigurationsparameter, die nicht zwischen den Cluster Member Systemen repliziert und synchronisiert werden:

- alle Einstellungen im Menü »System«
- das SSL-Device Zertifikat im Menü »SSL«
- die Systemlizenz und die Registrierungsdaten des Systems

Die Log-Dateien und Statistiken in den Menüs »Logs«, »Webmail Logs« und »Statistik« sind ebenfalls systemspezifisch und werden nicht repliziert. Alle anderen Konfigurationsparameter werden zwischen den Cluster Member Systemen repliziert und bei jeder Veränderung synchronisiert.

6.10.6.5 Einrichten der SEPPmail Cluster Systeme

Das erste SEPPmail-System eines Clusters muß vollständig eingerichtet sein. Siehe Kapitel Inbetriebnahme von SEPPmail 14

Das zweite SEPPmail-System muß mit den Basiseinstellungen eingerichtet werden. Dies beinhaltet die Netzwerkkonfiguration und die Registrierung des Systems. Siehe Kapitel Einrichten der Basiseinstellungen eines SEPPmail Systems 139

6.10.6.6 Cluster-Identifizierung herunterladen

Eine Cluster-Identifizierung wird benötigt, um ein weiteres SEPPmail-System zu einem bestehenden Clusterverbund hinzuzufügen oder einen Clusterverbund aus zwei SEPPmail-Systemen zu bilden.

Um eine Cluster-Identifizierung herunterzuladen, wählen Sie in der Konfigurationsoberfläche das Menü »Cluster«. Wählen Sie anschließend die Schaltfläche »Download Cluster Identifier« in der Sektion »Prepare for Cluster«. Sie erhalten danach einen »Datei speichern« Dialog und können die Cluster-Identifizierung als Datei »clusterid.txt« lokal speichern.

Abbildung 1 - Cluster-Identifizierung herunterladen

Abbildung 2 - Cluster-Identifizierung herunterladen und lokal speichern

6.10.6.7 SEPPmail Cluster einrichten

Zum Einrichten eines SEPPmail-Cluster benötigen Sie mindestens zwei Systeme. Grundsätzlich gibt es für die Anzahl der Cluster Member Systeme keine Beschränkung. Sie können ohne weiteres 10 Systeme oder mehr in einem Clusterverbund betreiben. Dieser Clusterverbund kann alle je nach spezifischer Anforderung so eingerichtet werden, dass alle 4 Betriebsarten Anwendung finden.

Die primäre Einrichtung eines SEPPmail-Cluster, bestehend aus mindestens zwei Systemen, funktioniert genauso wie das Hinzufügen weiterer Cluster Member Systeme.

Um eine SEPPmail-Appliance zu einem bestehenden Cluster hinzuzufügen (oder um ein Cluster erstmalig einzurichten), wählen Sie in der Konfigurationsoberfläche den Menüpunkt »Cluster«.

Zum Aufbau des Clusters müssen die Felder in der Sektion »Add this device to existing cluster« ausgefüllt werden. Gehen Sie dabei wie folgt vor:

1. Wählen Sie für den Parameter »Cluster Identifier« die Datei mit der Cluster-Identifizierung aus, welche Sie heruntergeladen haben.
2. Geben Sie für den Parameter »Cluster Member IP« die (physische) IP-Adresse der ersten SEPPmail-Appliance ein, zu welchem Sie dieses System hinzufügen möchten. Befinden sich schon mehrere Appliances im Cluster, so reicht die (physische) IP-Adresse eines Cluster Members Systems.
3. Geben Sie für den Parameter »IP address of this device« die eigene (physische) IP-Adresse ein, unter der diese Appliance für andere Appliances im Cluster erreichbar ist.
4. Überprüfen Sie alle zuvor eingegebenen Werte. Schließen Sie den Vorgang durch auswählen der Schaltfläche »start« ab. Der Clusterverbund wird nun erstellt bzw. erweitert, indem die bestehende Cluster Konfiguration auf das neue Cluster Member System repliziert wird. Alle nun folgenden Änderungen der Konfiguration im Cluster werden mit dem neu hinzugefügten Cluster Member System sofort automatisch synchronisiert.

Abbildung 1 - Hinzufügen einer SEPPmail Appliance zu einem bestehenden Cluster bzw. erstmaliges Erzeugen eines Clusters

Nachdem der Clusterverbund erstellt wurde ändert sich die Anzeige im Menü »Cluster« und es wird nun der Status des Clusterverbunds angezeigt. Wenn Sie dieses System aus dem Clusterverbund wieder entfernen möchten, so wählen Sie in der Sektion »remove from cluster« die Schaltfläche »remove this device from cluster«.

SEPPMAIL SWISS E-MAIL SECURITY

Login - Home - System - Mail System - Mail Processing - SSL - CA - Administration - Cluster - Logs - Webmail Logs - Statistics
Users - Groups - Webmail accounts - PGP public keys - X.509 Certificates - X.509 Root Certificates - Domain keys

Cluster Configuration

Prepare for Cluster	use this key to add a different device to this device/cluster Download Cluster Identifier
cluster members	Device ID: 0000-0000-0002, IP Address: 10.10.0.10, Port: 22, Status: OK
remove from cluster	remove this device from clu

Tue Jun 21 04:18:33 CEST 2011

Abbildung 2 - Cluster Status des 1. Cluster Member Systems

SEPPMAIL SWISS E-MAIL SECURITY

Login - Home - System - Mail System - Mail Processing - SSL - CA - Administration - Cluster - Logs - Webmail Logs - Statistics
Users - Groups - Webmail accounts - PGP public keys - X.509 Certificates - X.509 Root Certificates - Domain keys

Cluster Configuration

Prepare for Cluster	use this key to add a different device to this device/cluster Download Cluster Identifier
cluster members	Device ID: 0000-0000-0001, IP Address: 10.10.0.9, Port: 22, Status: OK
remove from cluster	remove this device from clu

Tue Jun 21 04:18:33 CEST 2011

Abbildung 3 - Cluster Status des 2. Cluster Member Systems

Wenn Sie ein SEPPmail-System einem bestehenden Clusterverbund hinzufügen oder erstmalig einen Clusterverbund erzeugen, so wird die gesamte bestehende Clusterkonfiguration auf dieses neue Cluster Member System repliziert und danach ständig mit dem Clusterverbund synchronisiert.

Alle Daten auf diesem System mit Ausnahme der Einstellungen in den Menüs »System« und »SSL« sowie den Log-Dateien und Statistiken in den Menüs »Logs«, »Webmail Logs« und »Statistics« gehen verloren.

Dies ist insofern wichtig, falls sich auf diesem System noch benötigte Konfigurationsdaten wie z.B. S/MIME Zertifikate, PGP Schlüssel, Secure Webmail Konten etc. befinden.

Weiterhin ist es sehr wichtig zu verstehen, in welcher Reihenfolge SEPPmail Systeme einem bestehenden Clusterverbund hinzugefügt werden müssen bzw. welches System die Replikationsquelle und welches System das Replikationsziel ist. Falls Sie diese Systeme beim Erstellen eines neues Clusterverbunds verwechseln so kann es passieren, dass ein bestehendes und eingerichtetes SEPPmail System mit den »leeren Daten« des neu hinzugefügten Systems überschrieben wird. Noch viel

wichtiger ist dies bei einem bestehenden Clusterverbund, wenn dieser bereits aus mehreren Cluster-Member-Systemen besteht. Das Verwechseln von Replikationsquelle und Replikationsziel bedeutet in diesem Fall, dass der bestehende Clusterverbund mit den »leeren Daten« des neuen Systems überschreiben wird.

Abbildung 4 - Schematische Darstellung der Replikation der Clusterkonfiguration zwischen zwei SEPPmail Cluster Member Systemen

Bis jetzt haben Sie die primäre Replikation und dann folgende Sychronisation der Konfigurationsdaten zwischen den Cluster Member Systemen eingerichtet. Um ein Hochverfügbarkeitscluster und ein Load Balancing Cluster einzurichten ist es erforderlich, die einzelnen Cluster Member Systeme unter einer oder mehreren virtuellen Cluster IP-Adressen zusammenzufassen.

6.10.6.8 Hochverfügbarkeitscluster einrichten

Zum Einrichten eines Hochverfügbarkeitsclusters sind zwei verschiedene Funktionen notwendig.

Im Menü »Cluster« in der Konfigurationsoberfläche ist die Replikation und dann folgende Sychronisation der Konfigurationsdaten der Clusterkonfiguration zwischen den Cluster Member Systemen einzurichten und zu aktivieren. Diesen Punkt haben wir bereits im vorherigen Kapitel behandelt.

Im Menü »System« in der Konfigurationsoberfläche sind die Überwachung der Cluster Member Systeme untereinander und die Prioritäten der einzelnen Cluster Member Systeme innerhalb des Clusters einzurichten.

Die Konfiguration der virtuellen Cluster IP-Adresse(n) erfolgt im Menüpunkt »System« (Advanced View) in der Sektion »IP ALIAS Adresses«. Diese Konfiguration muß in jedem Cluster Member System vorgenommen werden, das zum Cluster gehört.

Bei der Konfiguration für den Betrieb als reines Hochverfügbarkeitscluster (Failover Cluster) wird in den Cluster Member Systemen die gleiche virtuelle Cluster IP-Adresse konfiguriert. Ein System muß dabei mit der Priorität »Primary« konfiguriert werden und ein System muß mit der Priorität »Backup« konfiguriert werden. Siehe Abbildung 1 und Abbildung 2. Wir verwenden die IP-Adressen aus der Darstellung im Kapitel Hochverfügbarkeitscluster[122].

Abbildung 1 - Hochverfügbarkeitscluster - virtuelle Cluster IP-Adresse des 1. SEPPmail Cluster Member Systems

Abbildung 2 - Hochverfügbarkeitscluster - virtuelle Cluster IP-Adresse des 2. SEPPmail Cluster Member Systems

Die beiden Cluster Member Systeme sind nun unter einer virtuellen Cluster IP-Adresse zusammengefaßt. Wird diese Cluster IP-Adresse angesprochen, so reagiert das System mit der Priorität »Primary«. Falls dieses System nicht verfügbar ist, so antwortet das System mit der Priorität »Backup«. Es wird ein automatischer Statuswechsel durchgeführt, falls das primäre System nicht verfügbar ist. Das System mit dem Status »Backup« erhält seinen ursprünglichen Status automatisch zurück, sobald das primäre System wieder verfügbar ist. In diesem Fall ist gewährleistet, dass im Fehlerfall ein- und ausgehende E-Mails weiterhin verarbeitet werden können und im E-Mail Datenfluss keine Störung auftritt.

Abbildung 4 - Hochverfügbarkeitscluster - automatischer Statuswechsel des sekundären Systems (das primäre Cluster Member System ist nicht verfügbar)

Somit ist die Clusterkonfiguration abgeschlossen. Beim Einsatz eines Clusters ist folgendes zu beachten:

- Beim Routing von E-Mails zum SEPPmail Cluster sollte immer die virtuelle Cluster IP-Adresse angesprochen werden.
- Im internen E-Mail Server und im externen MTA müssen alle IP Adressen des Clusters berechtigt sein, E-Mails zuzustellen, d.h. alle physischen und virtuellen IP-Adressen des SEPPmail Cluster (E-Mail Relay Einstellungen der jeweiligen Komponenten).
- In der Firewall müssen alle IP-Adressen des Clusters berechtigt werden, eine SSH Verbindung (Port TCP/22) zum Update Server im SEPPmail Rechenzentrum aufzubauen, d.h. alle physischen und virtuellen IP-Adressen des SEPPmail Clusters.
- In einem Cluster werden die Konfigurationen der beiden SEPPmail Systeme automatisch synchronisiert (mit Ausnahme der Einstellungen im Menü »System«)

6.10.6.9 Load Balancing Cluster einrichten

Das zusätzliche Einrichten eines Load Balancing Clusters erfordert ein bereits funktionsfähig eingerichtetes Hochverfügbarkeitscluster. Ein Load Balancing Cluster teilt den Datenfluss für ein- und ausgehende E-Mails auf je ein Cluster Members System aus und ermöglicht eine optimale Auslastung der vorhandenen Systemressourcen.

Jede Gruppe von Cluster Member Systemen erhält zusätzlich zu den einzelnen physischen IP-Adressen der Einzelsysteme eine virtuelle IP-Adresse. In Abhängigkeit der zugewiesenen Priorität werden die Systeme beim Ansprechen der virtuellen Cluster IP-Adresse reagieren. Haben zwei oder mehr Cluster Member Systeme die gleiche Priorität im Clusterverbund, so werden die Systeme in der Reihenfolge antworten in der diese gestartet wurden.

In dieser Dokumentation wird ein Clusterverbund aus zwei SEPPmail Systemen gezeigt. Sie können ebenfalls ein Cluster aus drei oder mehr Systemen einrichten. In diesem Fall ist jede virtuelle Cluster IP-Adresse als zusätzliche IP Alias Adresse anzulegen.

Bei der Konfiguration für den Betrieb als Hochverfügbarkeitscluster (Failover Cluster) mit Aufteilung des ein- und ausgehenden E-Mail Datenflusses (Load Balancing Cluster) werden in den Cluster Member Systemen mindestens zwei virtuelle Cluster IP-Adresse konfiguriert.

Eine virtuelle Cluster IP-Adresse für den eingehenden E-Mail Datenfluss (IP Alias 0) und eine weitere virtuelle Cluster IP-Adresse (IP Alias 1) für den ausgehenden E-Mail Datenfluss. Damit ist beim Ausfall eines Cluster Member Systems gewährleistet, dass das zweite System die Funktion des ausgefallenen Systems mit übernehmen kann. Ein Cluster Member System muß dabei mit der Priorität »Primary« konfiguriert werden und ein Cluster Member System mit der Priorität »Backup«. Die Prioritäten müssen je virtueller IP-Adresse entgegengesetzt vergeben werden.

Jedem Cluster Member System sind nun jeweils zwei (oder auch mehr, falls z.B. 3 Systeme verwendet werden) IP Alias Adressen als virtuelle Cluster IP-Adressen zugeordnet. Die einzelnen Cluster Member Systeme reagieren je nach eingerichteter Priorität auf jeweils eine virtuelle Cluster IP-Adresse. Fällt ein System aus, so kann das verbleibende System immer als Backup System arbeiten.

Zusätzlich muß für jede virtuelle Cluster IP-Adresse eine eindeutige »Virtual Host ID« vergeben werden, da wir mehr als eine Alias IP-Adresse pro Cluster Member System gebunden haben. (die »VHID« muß für die entsprechende virtuelle Cluster IP-Adresse auf jedem System identisch sein)

Abbildung 5 - Hochverfügbarkeitscluster mit zusätzlicher Lastverteilung - zwei virtuelle Cluster IP-

Adressen des 1. SEPPmail Cluster Member Systems

Abbildung 6 - Hochverfügbarkeitscluster mit zusätzlicher Lastverteilung - zwei virtuelle Cluster IP-Adressen des 2. SEPPmail Cluster Member Systems

Somit ist die Clusterkonfiguration abgeschlossen. Beim Einsatz eines Clusters ist folgendes zu beachten:

- Beim Routing von E-Mails zum SEPPmail Cluster sollte immer die virtuelle Cluster IP-Adresse angesprochen werden.
- Im internen E-Mail Server und im externen MTA müssen alle IP Adressen des Clusters berechtigt sein, E.Mails zuzustellen, d.h. alle physischen und virtuellen IP-Adressen des SEPPmail Cluster (E-Mail Relay Einstellungen der jeweiligen Komponenten).
- In der Firewall müssen alle IP-Adressen des Clusters berechtigt werden, eine SSH Verbindung (Port TCP/22) zum Update Server im SEPPmail Rechenzentrum aufzubauen, d.h. alle physischen und virtuellen IP-Adressen des SEPPmail Clusters.
- In einem Cluster werden die Konfigurationen der beiden SEPPmail Systeme automatisch synchronisiert (mit Ausnahme der Einstellungen im Menü »System«)

6.10.6.10 Geo Cluster einrichten

Mit einem Geo Cluster können lokale SEPPmail Cluster die sich an mehreren unterschiedlichen geografischen Standorten eines Unternehmens befinden ihre Konfigurationsdaten automatisch synchronisieren.

Betrachten wir beim Einsatz eines Geo Cluster folgendes Szenario:

Ein Unternehmen kann neben der Firmenzentrale noch weitere geografisch getrennte Standorte besitzen und zwischen diesen Standorten via VPN verbunden sein. Die interne Kommunikation im Unternehmen wird über ein unternehmensweites Groupware System abgebildet.

Jeder geografische Standort hat z.B. einen eigenen Internetzugang für den lokalen Empfang und Versand von E-Mails. Jeder Standort betreibt eigene Groupware Server die untereinander miteinander verbunden sind. Die unternehemensinterne E-Mail Kommunikation wird über dieses eigene E-Mail Transportnetzwerk abgebildet.

Jeder geografische Standort kann seine E-Mails über einen eigenen Internetzugang versenden und empfangen. Ein dynamisches E-Mail Routing ermöglicht es, dass E-Mails grundsätzlich an allen Standorten durch das unternehmensinterne E-Mail Transportnetzwerk versendet oder empfangen werden können. Dies erfordert an jedem Standort jeweils ein eigenes SEPPmail Cluster zur E-Mail Signatur und zur Ver- und Entschlüsselung von E-Mails.

Die an jedem Standort lokal eingerichteten SEPPmail Cluster sind jeweils als Hochverfügbarkeitscluster eingerichtet. Jedes Cluster an den verschiedenen Standorten wäre somit ein eigenständiges und aber lokal begrenztes System, indem sich die Cluster Member Systeme gegenseitig überwachen und ihre Konfiguration untereinander synchronisieren.

Um zusätzlich eine globale Synchronisierung der einzelnen Cluster Systeme zwischen den geografisch getrennten Standorten einzurichten, können wir ein Geo Cluster oder auch »MultiSite System« einrichten. Ein Geo Cluster synchronisiert die Konfigurationen zwischen den einzelnen lokalen Cluster Systemen der geografische getrennten Standorte zu einem globalen SEPPmail Cluster System. Ein solches System wird als Geo Cluster bezeichnet. Es verbindet alle lokalen Cluster Systeme der geografisch getrennten Standorte zu einem unternehmensweiten Geo Cluster.

In diesem Geo Cluster werden alle Konfigurationsänderungen die an einem SEPPmail Cluster Member System durchgeführt werden sofort auf alle Cluster Member Systeme in allen Standorten automatisch synchronisiert. Damit ist gewährleistet, dass zu jedem Zeitpunkt die benötigten Daten wie z.B. neue Benutzerkonten incl. Benutzerzertifikaten oder Secure Webmail Konten auf allen Cluster Member Systemen zur Verfügung stehen. Eine manuelle Konfiguration jedes einzelnen Systems bzw. eine manuelle Synchronisation der Konfiguration zwischen den Cluster Member Systemen ist nicht mehr notwendig und reduziert den administrativen Konfigurationsaufwand.

Wie wird ein Geo Cluster eingerichtet?

Bei der Einrichtung eines Geo Clusters wird ein Cluster Member System am Standort B zu einem Cluster Member System vom Standort A hinzugefügt. Diese Cluster Member Systeme werden nicht über eine virtuelle Cluster IP-Adresse verbunden, wie das Hochverfügbarkeits- und Load Balancing Cluster. Es erfolgt lediglich die Synchronisation der Konfigurationsdaten.

Verfahren Sie hierzu wir in den Kapiteln Cluster-Identifizierung herunterladen 140 und SEPPmail Cluster einrichten 141.

6.10.6.11 Frontend-Backend Cluster einrichten

Falls Sie ein neu hinzugefügtes SEPPmail System aus Sicherheitsgründen ohne lokale Datenbank (z.B. Benutzerzertifikate, Domainzertifikate etc.) betreiben möchten, können Sie das neue System alternativ als Frontend-Server hinzufügen. Die eigentlichen Konfigurations- und Benutzerdaten liegen dabei auf den übrigen SEPPmail Systemen, die als Backend-Server Appliances operieren. Wählen Sie dazu in der Konfigurationsoberfläche den Menüpunkt »Cluster«.

Zum Hinzufügen des neuen SEPPmail Systems als Frondend-Server zu einem bestehenden Cluster müssen die Felder in der Sektion »Add this device as frontend server (no local database)« ausgefüllt werden. Gehen Sie dabei wie folgt vor:

1. Wählen Sie für den Parameter »Cluster Identifier« die Datei mit der Cluster-Identifizierung aus, welche Sie heruntergeladen haben. Siehe Abschnitt Cluster-Identifizierung herunterladen 140.
2. Geben Sie für den Parameter »Existing Appliance IP« die physische IP-Adresse des Cluster Member Systems bzw. die Alias IP-Adresse des bestehenden Clusterverbunds an, zu welchem Sie eine Verbindung aufbauen möchten.
3. Überprüfen Sie alle zuvor eingegebenen Werte. Schließen Sie den Vorgang durch auswählen der Schaltfläche »start« ab.

Auf den Backend-Servern ist keine Anpassung notwendig.

Abbildung 1 - Hinzufügen einer SEPPmail Appliance als Frondend-Server zu einem bestehenden Cluster Member System bzw. dem Clusterverbund

6.11 Menüpunkt "Logs"

Wählen Sie den Menüpunkt »Logs« zum Verwalten der E-Mail Log-Dateien und um die Log-Informationen der letzten 500 E-Mail-Bewegungen anzuzeigen. Die letzten E-Mail-Bewegungen sind in der Sektion »Mail Log (last 500)« aufgelistet.

Sektionen	Beschreibung
Other Logs	Anzeige zusätzlicher Log-Dateien
Queue Control	Anzeige der E-Mail-Warteschlange, Abarbeiten der aktuellen E-Mail-Warteschlange
Log Archive	Herunterladen und Löschen von Logdateien
Filter	Suche in bestehenden Logdateien
Mail Log (last 500)	Anzeige der letzen 500 Logeinträge in der E-Mail-Logdatei

Sektion »Other Logs«

Schaltfläche »Show webmail log...«

Anzeige der Log-Informationen für Nachtichten die via GINA-Technologie versendet wurden.

Schaltfläche »Show Blacklist / Greylist Log...«

Anzeige der Log-Informationen für eingehende E-Mails die durch Blacklisten-Bewertung vollständig oder durch Greylisting temporär abgewiesen wurden.

Sektion »Queue Control«

Siehe E-Mails in der Warteschlange anzeigen 152

Schaltfläche »Show queued mails...«

Wählen Sie die Schaltfläche »Show queued mails...«, um anzuzeigen welche E-Mails sich derzeit noch in der Warteschlage befinden.

Schaltfläche »Retry to deliver queued mails...«

Wählen Sie die Schaltfläche »Retry to deliver queued mails...«, um den Versand von E-Mails in der Warteschlange auszulösen.

Sektion »Log Archive«

Schaltfläche »Download complete log«

Wählen Sie die Schaltfläche »Download complete log«, um die komplette E-Mail Log-Datei einzusehen. In der aktuellen E-Mail Log-Datei sind alle aktuellen sowie archivierten Log-Informationen enthalten.

Schaltfläche »Download log archive«

Wählen Sie die Schaltfläche »Download log archive«, um alle archivierten Log-Informationen einzusehen.

Schaltfläche »Delete log archive«

Wählen Sie die Schaltfläche »Delete log archive«, um die das Log-Archive zu löschen.

Sektion »Filter«

In diesem Eingabefeld geben Sie die Werte ein nach denen die Log-Dateien durchsucht werden sollen. Als Ergebnis erhalten Sie eine Übersicht mit den Log-Informationen die den eingegebenen Filterwerten entsprechen.

Wählen Sie zusätzlich die Option »Include recently archived logs« aus, so werden auch kürzlich archivierte Log-Informationen in die Suche einbezogen.

Um den Filter auf alle archivierten Log-Dateien anzuwenden, wählen Sie die Option »Include complete archived logs (might be time-consuming)«. Dies kann je nach Größe der archivierten Log-Dateien einige Zeit bis zum Anzeigen des Ergebnis in Anspruch nehmen.

Sektion »Mail log (last 500)«

In dieser Sektion können Sie die Log-Datei Einträge der letzten 500 E-Mail Bewegungen einsehen. Dies ist der schnellste und gebräuchlichste Weg Log-Informationen einzusehen.

Farbcode für den momentanen Verarbeitungsstatus einer E-Mail:

black : Die E-Mail wurde noch nicht verarbeitet oder wurde direkt ausgeliefert.
green : Die E-Mail wurde erfolgreich ausgeliefert.
yellow : Die E-Mail konnte noch nicht erfolgreich ausgeliefert werden, dieser Vorgang wird in Intervallen wiederholt.
red : Die E-Mail konnte nicht ausgeliefert werden und wurde zurückgewiesen.

Den Verarbeitungsstatus einer E-Mail können Sie in der Spalte »To« (Empfänger E-Mail Adresse) einsehen. Die Empfänger E-Mail Adresse wird entsprechend den oben aufgeführten Farbcodes dargestellt. So haben Sie sehr schnell die Möglichkeit Abweichungen in der Verarbeitung von ein- und ausgehenden E-Mails zu erkennen.

Die letzten E-Mail Bewegungen werden mit folgenden Details angezeigt:

Parameter	Beschreibung
Nr.	Eine fortlaufende Nummerierung der E-Mail Nachrichten. Der Wert dieser Spalte ist farbig dargestellt und dient ebenfalls als Link zur Detailansicht der Log-Informationen. Wählen Sie diesen Link und Sie können die gesamten Log-Informationen zu dieser E-Mail einsehen.
Source IP	IP-Adresse des E-Mail Absenders. Die IP-Adresse beschreibt den E-Mail-Server, der die E-Mail direkt an SEPPmail gesendet hat. (Hier ist nicht der jeweilige Arbeitsplatzrechner gemeint.)

Parameter	Beschreibung
Date	Versanddatum der E-Mail
From	Absender E-Mail-Adresse
To	Empfänger E-Mail-Adresse
Message-ID	Eindeutige Kennung der E-Mail
Subject	Betreffzeile der jeweiligen E-Mail
Size	Größe der E-Mail

6.11.1 E-Mails in der Warteschlange anzeigen

Menü »Logs«

E-Mails die sich aktuell in der lokalen SEPPmail E-Mail-Warteschlange (Mail-Queue) befinden werden durch klicken der Schaltfläche »Show queued mails...« angezeigt.

Parameter	Beschreibung
ID	Eindeutige Kennung der jeweiligen Nachricht
Date	Datum, an welchem die entsprechende E-Mail versandt wurde
Size	Grösse der E-Mail
From	Absender E-Mail Adresse
To	Empfänger E-Mail Adresse
Status	Der aktuelle Status der E-Mail-Verarbeitung

6.12 Menüpunkt "Statistics"

Menü »Statistics«

In der Übersicht werden die Statistiken für Durchsatz, Technologie, AntiSPAM, Prozessor und Speicher-Statistiken dargestellt. Diese Statistiken werden für die Zeitabschnitte Heute, Letzte Woche, Letzten Monat, Letztes Jahr und die letzten 3 Jahre angezeigt.

Sektion »Throughput Visualisation«

Sie sehen die Anzahl versendeter und empfangener Nachrichten und die Anzahl der durchgeführten Ver- und Endschlüsselungsoperationen. Zusätzlich sehen Sie die Anzahl der Nachrichten die im Durchschnitt verarbeitet wurden und wie groß die maximale Anzahl verarbeiteter Nachrichten pro Minute in der entsprechenden Betrachtungsperiode war.

Parameter	Beschreibung
Today	Durchsatz-Statistiken für den folgenden Zeitabschnitt: heute
Last Week	Durchsatz-Statistiken für den folgenden Zeitabschnitt: Letzte Woche
Last Month	Durchsatz-Statistiken für den folgenden Zeitabschnitt: Letzten Monat
Last Year	Durchsatz-Statistiken für den folgenden Zeitabschnitt: Letztes Jahr
Last 3 Years	Durchsatz-Statistiken für den folgenden Zeitabschnitt: Letzte 3 Jahre

Sektion »Technology Visualisation«

Sie sehen die Anzahl verarbeiteter E-Mails getrennt nach den Typen Secure Webmail, S/MIME-, OpenPGP- und Domainverschlüsselung. Zusätzlich sehen Sie, die Anzahl der Nachrichten die im Durchschnitt verarbeitet wurden und wie groß die maximale Anzahl verarbeiteter Nachrichten pro Minute in der entsprechenden Betrachtungsperiode war.

Parameter	Beschreibung
Today	Technologie-Statistiken für den folgenden Zeitabschnitt: heute
Last Week	Technologie-Statistiken für den folgenden Zeitabschnitt: Letzte Woche
Last Month	Technologie-Statistiken für den folgenden Zeitabschnitt: Letzten Monat
Last Year	Technologie-Statistiken für den folgenden Zeitabschnitt: Letztes Jahr
Last 3 Years	Technologie-Statistiken für den folgenden Zeitabschnitt: Letzte 3 Jahre

Sektion »Spam Visualisation«

Sie sehen die Anzahl erhaltener Nachrichten, die Anzahl der SPAM-Erkennungen und die Anzahl der E-Mails die anhand von Black- oder Greylisting behandelt wurden. Zusätzlich sehen Sie die Anzahl der SPAM-Nachrichten die im Durchschnitt verarbeitet wurden und wie groß die maximale Anzahl verarbeiteter SPAM-Nachrichten pro Minute in der entsprechenden Betrachtungsperiode war.

Parameter	Beschreibung
Today	SPAM-Statistiken für den folgenden Zeitabschnitt: heute
Last Week	SPAM-Statistiken für den folgenden Zeitabschnitt: Letzte Woche
Last Month	SPAM-Statistiken für den folgenden Zeitabschnitt: Letzten Monat
Last Year	SPAM-Statistiken für den folgenden Zeitabschnitt: Letztes Jahr
Last 3 Years	SPAM-Statistiken für den folgenden Zeitabschnitt: Letzte 3 Jahre

Sektion »CPU Usage Visualisation«

Sie sehen die Prozessorauslastung getrennt nach Systemverarbeitung, Verarbeitung im User Mode (Ausführung von Applikationen) und Prozessen die bezüglich Prozesspriorität durch das nice-Dienstprogramm gesteuert wurden.

Parameter	Beschreibung
Today	Statistiken zur Prozessor-Auslastung für den folgenden Zeitabschnitt: heute
Last Week	Statistiken zur Prozessor-Auslastung für den folgenden Zeitabschnitt: Letzte Woche
Last Month	Statistiken zur Prozessor-Auslastung für den folgenden Zeitabschnitt: Letzten Monat
Last Year	Statistiken zur Prozessor-Auslastung für den folgenden Zeitabschnitt: Letztes Jahr
Last 3 Years	Statistiken zur Prozessor-Auslastung für den folgenden Zeitabschnitt: Letzte 3 Jahre

Sektion »Memory Usage Visualisation«

Sie sehen die aktive und totale Auslastung des Arbeitsspeichers, Speicherauslagerungen sowie freie Kapazitäten des Arbeitsspeichers.

Parameter	Beschreibung
Today	Arbeitsspeicher-Statistiken für den folgenden Zeitabschnitt: heute
Last Week	Arbeitsspeicher-Statistiken für den folgenden Zeitabschnitt: Letzte Woche
Last Month	Arbeitsspeicher-Statistiken für den folgenden Zeitabschnitt: Letzten Monat
Last Year	Arbeitsspeicher-Statistiken für den folgenden Zeitabschnitt: Letztes Jahr
Last 3 Years	Arbeitsspeicher-Statistiken für den folgenden Zeitabschnitt: Letzte 3 Jahre

6.13 Menüpunkt "Users"

Wählen Sie den Menüpunkt »Users«, um die internen Benutzer der SEPPmail Appliance zu verwalten.

Folgende Vorgänge werden in den kommenden Abschnitten beschrieben:

Übersicht 156
Benutzer erstellen 156
Benutzer verwalten 157

6.13.1 Übersicht Menüpunkt "Users"

Parameter	Beschreibung
User ID	Name des Benutzerkontos zur Anmeldung an der SEPPmail Konfigurationsoberfläche.
Name	Tatsächlicher Benutzername, z.B. Robert Lander
E-Mail	E-Mail Adresse des Benutzer
PGP	Anzahl der im Benutzerkonto installierten PGP Benutzerschlüssel
S/MIME	Anzahl der im Benutzerkonto installierten S/MIME Benutzerzertifikate
State	Aktueller administrativer Status des Benutzer

6.13.2 Interne Benutzer erstellen

Menü »Users«

Zum Erstellen eines neuen Benutzerskontos wählen Sie die Schaltfläche »Create new user account...«.

Füllen Sie folgende Felder aus, um den Benutzer zu erstellen:

Parameter	Beschreibung
User ID	Benutzer-ID
Full Name	Vollständiger Name des Benutzers
E-Mail	E-Mail-Adresse des Benutzers
Password	Kennwort des Benutzers

Parameter »User ID«

Erfassen Sie in diesem Feld die Benutzer-ID des Benutzers, z.B. die E-Mail-Adresse oder einen anderen eindeutigen Wert. Benötigt wird diese ID zum Anmelden an der Konfigurationsoberfläche.

Parameter »Full Name«

Vollständiger Name des Benutzers, z.B. Robert Lander

Hinweis:

Geben Sie den vollständigen Namen des Benutzers unbedingt ein, da dieser Wert beim Erstellen von Benutzerzertifikaten erforderlich ist.

Parameter »E-Mail«

Erfassen Sie in diesem Feld die E-Mail-Adresse des Benutzers. Anhand dieser E-Mail-Adresse werden geprüft, ob ein Absender berechtigt ist die Cryptofunktion von SEPPmail zu nutzen. Für alle Absender die kein Benutzerkonto haben wird die Cryptofunktion nicht angewendet.

Parameter »Password«

Erfassen Sie in diesem Feld das Kennwort des Benutzers (geben Sie dieses zwei Mal ein).

Hinweis:

Ein Passwort für den Benutzer wird nur dann benötigt, wenn dieser administrative Berechtigung an der Konfigurationsoberfläche erhalten soll. Die Berechtigung, für den Zugriff auf bestimmte Menüpunkte, kann durch die Auswahl der Gruppen definiert werden.

6.13.3 Interne Benutzer verwalten

Menü »Users«

Um die Details eines Benutzers zu bearbeiten, klicken Sie auf die »User ID« des entsprechenden Benutzers.

Sektion »User Data«

Parameter	Beschreibung
User ID	eindeutige Benutzer-ID
Full Name	vollständiger Name des Benutzers (editierbar)
E-Mail	E-Mail-Adresse des Benutzers (muss eindeutig sein)
Password	Kennwort des Benutzers
Encryption Settings	administrativer Status des Benutzerkontos

Parameter	Beschreibung
Notification Settings	Lesebestätigung für GINA-Nachrichten
User Statistics	statistische Übersicht des Systembenutzung

Parameter »User ID«

Benutzer-ID des Benutzers, z.B. die E-Mail-Adresse oder ein anderer eindeutiger Wert. Dieser Parameter ist Read-Only und kann nachträglich nicht mehr verändert werden. Die Benutzer-ID ist der Anmeldename des Benutzers für den Zugang zur Konfigurationsoberfläche.

Parameter »Full Name«

Vollständiger Name des Benutzers. Dieser Parameter kann nachträglich verändert werden.

Hinweis:

Geben Sie den vollständigen Namen des Benutzers unbedingt ein, da dieser Wert beim Erstellen von Benutzerzertifikaten erforderlich ist.

Parameter »E-Mail«

E-Mail-Adresse des Benutzers. Dieser Parameter ist Read-Only und kann nachträglich nicht mehr verändert werden.

Parameter »Password«

Das Kennwort des Benutzers kann hier neu vergeben werden.

Hinweis:
Ein Passwort für den Benutzer wird nur dann benötigt, wenn dieser administrative Berechtigung an der Konfigurationsoberfläche erhalten soll. Die Berechtigung, für den Zugriff auf bestimmte Menüpunkte, kann durch die Auswahl der Gruppen definiert werden.

Parameter »Encryption Settings«

Hier können Sie den administrativen Status des Benutzerkontos beeinflussen. Sie können die Cryptofunktionen des Benutzers durch die folgenden Optionen einschränken oder wieder freigeben.

1. May not encrypt mails : deaktiviert das verschlüsseln ausgehender E-Mails für diesen Benutzer
2. May not sign mails : deaktiviert das signieren ausgehende E-Mails für diesen Benutzer

Wenn Sie beide Optionen aktivieren, dann wird das Benutzerkonto deaktiviert. Der Benutzer kann in diesem Fall die Cryptofunktionen für ausgehende E-Mails nicht mehr nutzen. Eingehende E-Mails werden weiterhin entschlüsselt. Durch das Deaktivieren des Benutzerkontos bleibt dieses in der Konfiguration erhalten, es wird aber keine Benutzerlizenz verbraucht.

Hinweis:

Benötigt ein Benutzer die Cryptofunktionen von SEPPmail nicht mehr und existiert für diesen Benutzer S/MIME oder OpenPGP Schlüsselmaterial, so empfehlen wir, das Benutzerkonto nicht zu löschen sondern zu deaktivieren. Die verbrauchte Benutzerlizenz wird dadurch wieder frei. Eingehende E-Mails für diesen Benutzer können weiterhin entschlüsselt werden.

Löschen Sie das Benutzerkonto mit existierenden Schlüsselmaterial, so wird ebenfalls eine verbrauchte Benutzerlizenz freigegeben. Eingehende E-Mails für diesen Benutzer können dann nicht mehr durch SEPPmail entschlüsselt werden. Das Benutzerzertifikat eines z.B. ausgeschiedenen Mitarbeiters kann bei externen Kommunikationspartnern weiterhin vorhanden sein und auch für die Verschlüsselung genutzt werden.

Parameter »Notification Settings«

Aktiviert das Versenden von Benachrichtigungen, wenn von diesem Benutzer versendete GINA-E-Mails vom Empfänger gelesen wurden. Dies bezieht sich auf alle GINA-E-Mails die dieser Benutzer versendet. Das Anfordern einer Lesebestätigung ist dann nicht mehr bei jeder ausgehenden GINA-E-Mails separat erforderlich. Dieser Parameter kann durch eine übergeordnete Einstellung innerhalb der E-Mail-Domain übersteuert werden.

Parameter »User Statistics«

Zeigt eine statistische Übersicht zu verarbeiteten E-Mail bzgl. dem Cryptoverfahren, der Anzahl und der letzen Aktivität.

Sektion »Group Memberships«

Zeigt an, in welchen Gruppen das Benutzerkonto Mitglied ist. Die Gruppenmitgliedschaft wird im Menü »Groups« verwaltet.

Sektion »S/MIME«

Schaltfläche/Parameter	Beschreibung
Import S/MIME Certificate...	vorhandenes S/MIME-Zertifikat importieren
Generate S/MIME Certificate...	neues S/MIME-Zertifikat für den Benutzer durch die SEPPmail-CA selbst generieren
Generate [CA] Certificate...	neues S/MIME-Zertifikat für den Benutzer über den eingerichteten CA-Connector beziehen
Serial	Seriennummer des Zertifikats
Certificate Authority	Subject der CA die dieses Zertifikat ausgestellt hat
Issued on	Ausstellungsdatum des Zertifikats

Schaltfläche/Parameter	Beschreibung
Expires on	Ablaufdatum des Zertifikats

Sektion »PGP«

Schaltfläche/Parameter	Beschreibung
Import PGP key...	vorhandenes PGP-Schlüsselpaar importieren
Generate new PGP key...	neues PGP-Schlüsselpaar für den Benutzer die SEPPmail selbst generieren
Key ID	Schlüssel-ID des Schlüsselpaars
User ID	Benutzer-ID des Schlüsselpaars
Issued on	Ausstellungsdatum des Schlüsselpaars
Expires on	Ablaufdatum des Schlüsselpaars

Sektion »Remote POP3«

Geben Sie die POP3-Authentifizierungsdetails des Benutzers ein, um E-Mails des Benutzers regelmässig von einem POP3-Server abzurufen.

Parameter	Beschreibung
User ID	Benutzername
Password	Kennwort
Mail server	IP-Adresse oder Hostname des POP3 E-Mail-Servers von dem E-Mails abgeholt werden sollen

6.14 Menüpunkt "Groups"

Wählen Sie den Menüpunkt »Groups«, um die Gruppenstruktur der SEPPmail Appliance zu verwalten.

Folgende Vorgänge werden in den kommenden Abschnitten beschrieben:

6.14.1 Übersicht Menüpunkt "Groups"

Wollen Sie zusätzlich zum Benutzer »admin« weiteren Benutzern administrative Rechte an der Konfigurationsoberfläche geben, so können Sie einen Benutzer zum Mitglied unterschiedlicher Gruppen machen. Die Gruppenstruktur entspricht im wesentlichen den einzelnen Menüpunkten.

Sie haben über den Menüpunkt »Groups« eine Übersicht aller den jeweiligen Gruppen zugeordneten Benutzern.

Eine Ausnahme bildet die folgende Gruppe:

»backup (Backup Operator)«. Sie dient nicht zur Vergabe von Berechtigungen an Menüpunkten der Konfigurationsoberfläche.

Gruppe	Beschreibung
	Wählen Sie die Schaltfläche »Create new user group...«, um eine neue Gruppe anzulegen. Siehe Gruppen erstellen 163. Gruppen die einmal angelegt wurden können nachträglich nicht mehr gelöscht werden.
admin (Administrator)	Alle Mitglieder dieser Gruppe sind dem Standardbenutzer »admin« gleichgestellt und haben uneingeschränkten administrativen Zugang zur Konfigurationsoberfläche mit allen Berechtigungen. Um einen Benutzer Sicherheitsäquivalent zum Standardbenutzer »admin« zu machen, fügen Sie diesen Benutzer der Gruppe »admin (Administrator)« hinzu.
administrationadmin (GUI Access to Administration Section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü »Administration« in der Konfigurationsoberfläche.
backup (Backup Operator)	Dieses Gruppe ist eine Sonderbedeutung zugeordnet. Sie unterscheidet sich von den Systemgruppen für den Zugriff auf die Konfigurationsoberfläche dadurch, dass kein Zugriff auf die Konfigurationsoberfläche erfolgt. Alle Mitglieder dieser Gruppe erhalten das Systembackup des jeweiligen Systems einmal täglich via E-Mail. Das Systembackup wird täglich um 0.00 Uhr erzeugt und via E-Mail an alle Mitglieder dieser Gruppe gesendet.
caadmin (GUI Access to CA	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü »CA« in der Konfigurationsoberfläche.

Gruppe	Beschreibung
Section)	
clusteradmin (GUI Access to Cluster Section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü »Cluster« in der Konfigurationsoberfläche.
domainkeysadmin (GUI Access to Domain Keys Section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü »Domain keys« in der Konfigurationsoberfläche.
groupsadmin (GUI Access to Groups Section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü »Groups« in der Konfigurationsoberfläche.
homeadmin (GUI Access to Home Section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü »Home« in der Konfigurationsoberfläche.
logsadmin (GUI Access to Logs Section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü »Logs« in der Konfigurationsoberfläche.
mailprocessingadmin (GUI Access to Mail Mail Processing Section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü »Mail Processing« in der Konfigurationsoberfläche.
mailsystemadmin (GUI Access to Mail System Section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü »Mail System« in der Konfigurationsoberfläche.
multiplecustomersadmin (Admin access to Customer settings in multitenant deployments)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü »Customers« in der Konfigurationsoberfläche.
pgpkeysadmin (GUI Access to PGP Keys Section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü »PGP public keys« in der Konfigurationsoberfläche.
ssladmin (GUI Access to SSL Section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü »SSL« in der Konfigurationsoberfläche.
statisticsadmin (GUI Access to Statistics Section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü »Statistics« in der Konfigurationsoberfläche. Zusätzlich erhalten alle Mitglieder dieser Gruppe einen täglichen System-Report des jeweiligen Systems. Der System-Report wird täglich um 0.00 Uhr erzeugt und via E-Mail an alle Mitglieder dieser Gruppe gesendet.
systemadmin (GUI Access to System Section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü »System« in der Konfigurationsoberfläche.

Gruppe	Beschreibung
usersadmin (GUI Access to Users Section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü »Users« in der Konfigurationsoberfläche.
webmailaccountsadmin (GUI Access to Webmail Accounts Section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü »Webmail accounts« in der Konfigurationsoberfläche.
x509certificatesadmin (GUI Access to X.509 Certificates Section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü »X.509 Certificates« in der Konfigurationsoberfläche.
x509rootcertificatesadm in (GUI Access to X.509 Root Certificates Section)	Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü »X.509 Root Certificates« in der Konfigurationsoberfläche.

6.14.2 Gruppen erstellen

Menü »Groups«

Zum Erstellen einer neuen Gruppe wählen Sie in der Konfigurationsoberfläche die Schaltfläche »Create new user group...«. Geben Sie den Namen der neuen Gruppe sowie eine kurze Beschreibung ein und wählen Sie dann die Schaltfläche »Create«, um die Erstellung der neuen Gruppe abzuschließen.

6.14.3 Gruppen verwalten

Menü »Groups«

Benutzer können je nach Rolle einer oder mehreren Gruppen zugeordnet werden.

Alle Mitglieder der Gruppe »backup« (Backup Operator)« erhalten das Systembackup des jeweiligen Systems einmal täglich via E-Mail. Das Systembackup wird täglich um 0.00 Uhr erzeugt und via E-Mail an alle Mitglieder dieser Gruppe gesendet. (Siehe Kapitel Backup User erstellen 24).

Die weiteren vordefinierten Gruppen ermöglichen deren Mitgliedern die Administration der SEPPmail-Appliance. Die Gruppe »webmailaccountsadmin« erlaubt beispielsweise den Zugriff auf den Menüpunkt »Webmail accounts« in der SEPPmail Konfigurationsoberfläche.

Für jeden Menüpunkt in der Konfigurationsoberfläche gibt es eine entsprechende Gruppe, jeweils vermerkt mit »GUI Access to...«. So können verschiedene Administrationsaufgaben an mehrere Personen übertragen werden.

Zum Löschen einer vorhandenen Gruppe wählen Sie die Schaltfläche »Edit ...« neben der Gruppe die Sie löschen wollen. Wählen Sie zum Löschen die Schaltfläche »Delete Group«.

6.14.4 Benutzer zuweisen und entfernen

Menü »Groups«

Um einen Benutzer einer bestehenden Gruppe hinzuzufügen, wählen Sie die Schaltfläche »Edit...« neben der Gruppe, der Sie einen Benutzer hinzufügen wollen.

Wählen Sie die im Bereich »Group members« einen Benutzer. Fügen Sie diesen Benutzer durch wählen der Schaltfläche »Add user...« der Gruppe hinzu. Wählen Sie zum Speichern des hinzugefügten Benutzer die Schaltfläche »Save changes«.

Um einen Benutzer aus einer Gruppe zu entfernen, markieren Sie den Benutzereintrag in der Liste » Group members« und wählen Sie zum Entfernen die Schaltfläche »Remove selected users...«.

6.15 Menüpunkt "GINA accounts"

Wählen Sie den Menüpunkt »GINA-Konten«, um die automatisch erzeugten Webmail-Konten der SEPPmail Appliance zu verwalten.

Folgende Vorgänge werden in den kommenden Abschnitten beschrieben:

Übersicht 165
GINA-Benutzerkonten sperren 167
GINA-Benutzerkonten löschen 167
GINA-Benutzerkonten verwalten 167

6.15.1 Übersicht Menüpunkt "GINA accounts"

Menü »GINA accounts«

Dieses Menü ist in mehrere Bereiche aufgeteilt die zum Teil dynamisch erzeugt werden. Dynamisch erzeugt bedeutet in diesem Zusammenhang, dass für jeden angelegten Kunden im Menü »Customer« eine eigene Sektion angezeigt wird. In dieser Sektion werden alle dem Kunden zugeordneten GINA-Benutzerkonten angezeigt.

Parameter	Beschreibung
[Kundenname]	Gruppierung für einen oder mehrere Kundenbereiche, in denen dem Kunden zugeordneten GINA-Benutzerkonten gruppiert werden.
Default Customer	GINA-Benutzerkonten die keinem anderen Kunden zugeordnet sind
No Customer	GINA-Benutzerkonten die nicht verwendet werden dürfen
E-mail	E-Mail-Adresse des Empfängers
Account status	Administrativer Status des GINA-Benutzerkontos
Last message status	Status der letzten Benutzerinteraktion mit Zeitstempel

Parameter »[Kundenname]«

Wird ein SEPPmail-System für mehrere Kunden gleichzeitig verwendet, so können einem Kunden spezifische Konfigurationsparameter explizit zugewiesen werden. Dies ist auch für GINA-Benutzerkonten der Fall. Für jeden im Menü »Customer« angelegten Kunden wird eine eigene Sektion angelegt die mit dem Kundennamen bezeichnet wird. Innerhalb dieses kundenspezifischen Bereichs werden alle dem Kunden zugeodeneten GINA-Benutzerkonten angezeigt. Ein externen GINA-Benutzer kann mehreren Kundensektionen zugeordnet sein.

Parameter »Default Customer«

Diese Sektion hat eine Sonderbedeutung. Sie enthält alle GINA-Benutzerkonten, die keiner anderen Kundensektion zugeordnet sind.

Parameter »No Customer«

Diese Sektion hat eine Sonderbedeutung. Sie enthält alle GINA-Benutzerkonten, die nicht mehr verwendet werden dürfen. Diese GINA-Benutzerkonten sind deaktiviert, bleiben aber in der Konfiguration erhalten. Sie können wieder reaktiviert werden, indem sie einem Kunden oder dem »Default Customer« zugeordnet werden.

Parameter »E-mail«

E-Mail Adresse des GINA-Empfängers

Parameter »Account status«

Administrativer Status des GINA-Benutzerkontos des Empfängers. Der »Account status« kann folgende Werte anzeigen:

locked	Das GINA-Benutzerkonto des Empfängers ist gesperrt.
enabled	Das GINA-Benutzerkonto des Empfängers ist aktiv.

Parameter »Last message status«

In dieser Spalte wird der Status der letzen Benutzerinteraktion angezeigt. Der »last message status« kann folgende Werte anzeigen:

<Statusmeldung> Wird eine Statusmeldung in rot angezeigt, dann wurde die letzte Benutzerinteraktion, z.B. die Benutzeranmeldung am GINA-Benutzerkonto, nicht erfolgreich ausgeführt.

Beispiele:

May 2 18:00:00: auth failure, pwdCount 4	Das Benutzerkennwort des Empfängers wurde 4 Mal falsch eingegeben.
May 2 18:00:00: auth failure, disable account	Das Benutzerkonto des Empfängers wurde gesperrt, nachdem das Benutzerkennwort 4 Mal falsch eingegeben wurde.

<Statusmeldung> Wird die Statusmeldung in grün angezeigt, dass wurde die letzte Benutzerinteraktion, z.B. das Lesen einer GINA-Nachricht, erfolgreich ausgeführt.

Beispiele:

May 2 18:00:00: success. message-ID: <4DA69716.8030601@customer.com>	Eine GINA-Nachricht wurde vom Empfänger erfolgreich entschlüsselt und angezeigt.

May 2 18:00:00: auth ok	Der Empfänger konnte sich erfolgreich an seinem GINA-Benutzerkonto anmelden.

6.15.2 GINA-Benutzerkonten sperren

Menü »GINA accounts«

Um GINA-Benutzerkonten zu sperren, klicken Sie in der Konfigurationsoberfläche auf den Menüpunkt » GINA accounts«. Klicken Sie anschließend auf die E-Mail-Adresse des entsprechenden GINA-Benutzers. Um das ausgewählte GINA-Benutzerkonto zu sperren, wählen Sie in der Sektion »User Data« im Bereich »Account status« auf die Option »locked«. Das Benutzerkonto ist nun gesperrt und kann nur durch einen Administrator entsperrt werden.

6.15.3 GINA-Benutzerkonten löschen

Menü »GINA accounts«

Um GINA-Benutzerkonten zu löschen, klicken Sie in der Konfigurationsoberfläche auf den Menüpunkt » GINA accounts«. Klicken Sie anschließend auf die E-Mail-Adresse des GINA-Benutzers. Um das ausgewählte Benutzerkonto zu löschen, klicken Sie auf die Schaltfläche »Delete Account«.

Wichtiger Hinweis:

Beim Erstellen eines GINA-Benutzerkontos wird ein eindeutiger Schlüssel zur Ver- und Entschlüsselung der GINA-Nachrichten erzeugt.

Alle GINA-Nachrichten für diesen Empfänger werden mit dem zu diesem GINA-Benutzerkonto gehörenden Schlüssel verschlüsselt und können nur mit diesem Schlüssel wieder entschlüsselt und gelesen werden.

Wird ein GINA-Benutzerkonto gelöscht, so wird ebenfalls der eindeutige Schlüssel für dieses Benutzerkonto gelöscht. Dies hat zur Folge, dass der Empfänger alle bisher empfangenen GINA-Nachrichten nicht mehr entschlüsseln und lesen kann.

Wird ein neues GINA-Benutzerkonto für einen zuvor gelöschten Empfänger angelegt, so wird ein neuer eindeutiger Schlüssel erzeugt. Der Empfänger kann nur GINA-Nachrichten entschlüsseln und lesen, die mit dem neuen Schlüssel verschlüsselt wurden. Alle GINA-Nachrichten die vor dem Erstellungszeitpunkt des neuen GINA-Benutzerkontos empfangen wurden, können nicht mehr entschlüsselt und gelesen werden. Dies ist unabhängig davon, ob ein neu angelegtes GINA-Benutzerkonto denselben Namen hat wie ein zuvor gelöschtes GINA-Benutzerkonto.

6.15.4 GINA-Benutzerkonten verwalten

Menü »GINA accounts«

Sektion »User Data«

Parameter	Beschreibung
Creation Info	Absender E-Mail-Adresse und Zeitstempel bei Erstellen des GINA-Benutzerkontos.
Name	Name des GINA-Empfängers.
E-Mail	E-Mail-Adresse des Empfängers.
Password reminder	Sicherheitsfrage bei Verlust des Benutzerkennworts. Frage und Antwort diesen zum Identifizieren des Empfängers.
Answer	Antwort auf die Sicherheitsfrage.
Password	Setzen eines neuen Benutzerkennworts.
Must Change Password	Wenn Sie diese Option setzen wird der GINA-Empfänger beim nächsten Login aufgefordert, sein Kennwort zu ändern.
Zip Attachement	GINA-Nachrichten werden innerhalb einer ZIP-Dateianlage gesendet.
Account status	Status des Benutzerkontos.
Password Security Level	
Mobile number	Mobilfunkrufnummer des Empfängers

Parameter »Creation Info«

Absender E-Mail-Adresse und Zeitstempel bei Erstellen des GINA-Benutzerkontos.

Parameter »Name«

Name des GINA-Empfängers. Diese Informationen kann der GINA-Empfänger innerhalb seines Benutzerkontos selbst verwalten.

Parameter »E-Mail«

E-Mail-Adresse des Empfängers.

Parameter »Password reminder«

Sicherheitsfrage bei Verlust des Benutzerkennworts. Frage und Antwort diesen zum Identifizieren des Empfängers.

Parameter »Answer«

Antwort auf die Sicherheitsfrage.

Parameter »Password«

Setzen eines neuen Benutzerkennworts.

Parameter »Must Change Password«

Wenn Sie diese Option setzen wird der GINA-Empfänger beim nächsten Login aufgefordert, sein Kennwort zu ändern.

Parameter »Zip Attachment«

Nutzen Sie diesen Parameter, wenn Sie möchten, dass GINA-Nachrichten in Form einer ZIP-Dateianlage zur GINA-Nachricht gesendet werden. Dieser Parameter ist bei Empfängern erforderlich, die Outlook Web Access (OWA) verwenden, da GINA-Nachrichten im Format einer HTML-Datei aus OWA nicht entschlüsselt werden können. Um die Einstellung nur bei einzelnen GINA-Nachrichten zu nutzen, kann das Tag »[owa]« in der Betreffzeile der E-Mail verwendet werden. Sollte eine GINA-Nachricht im Format einer HTML-Datei an einen OWA-Empfänger gelangen, erkennt die SEPPmail-Appliance dies. Der Absender wird daraufhin aufgefordert, die E-Mail nochmal zu senden. Gleichzeitig wird im GINA-Benutzerkonto des Empfängers der Parameter »ZIP Attachment« automatisch gesetzt. Bei allen neu gesendeten GINA-Nachrichten werden die GINA-Nachrichten innerhalb einer ZIP-Dateianlage gesendet und können via Outlook Web Access dargestellt werden.

Parameter »Account status«

locked	Webmail-Konto ist deaktiviert/gesperrt
enabled	Webmail-Konto ist aktiviert

Diese Option wird verwendet, um Brute-Force* Angriffe zu vermeiden. Das GINA-Benutzerkonto wird automatisch deaktiviert, nachdem das Kennwort 4 Mal falsch eingegeben wurde. Das Benutzerkonto wird solange gesperrt, bis es durch den Administrator wieder freigegeben wird.

Parameter »Password Security Level«

Wählen Sie das Verfahren für den Kennwort-Reset, damit ein externer GINA-Benutzer sein GINA-Benutzerkennwort zurücksetzen kann. Danach wird je nach ausgewählem Verfahren für den Kennwort-Reset eines der folgenden Verfahren verwendet:

Auswahlwert »default (Reset by hotline)«

Der Wert »default« bezieht sich auf die für die jeweilige GINA-Domain ausgewählte globale Standardeinstellung. Dieses wird innerhalb der Konfiguration der GINA-Domain in der Sektion »Security« eingestellt.

Auswahlwert »Reset by Email verification«

Der externe GINA-Benutzer kann sein Kennwort selbstständig zurücksetzen. Zur Aktivierung und Bestätigung dieser Aktion erhält er eine E-Mail-Benachrichtigung mit einem Aktivierungslink. Nach dem Bestätigen dieses Aktivierungslinks wird das vom externen Benutzer zuvor neu eingegebene Kennwort aktiviert. Ein Login mit dem neu gesetzten Kennwort ist nun möglich.

Auswahlwert »Reset by hotline«

Der externe GINA-Benutzer kann sein Kennwort nicht selbstständig zurücksetzen. Er gibt dazu seine Rufnummer an, unter der er für den Support erreichbar ist. Nach Überprüfung durch die Sicherheitsfrage erhält er vom Support-Mitarbeiter ein neues Einmalkennwort zum nächsten Login. Nach dem Login ist es erforderlich, ein neues persönliches Kennwort erfassen. Ein Login mit dem neu gesetzten Kennwort ist nun möglich.

Auswahlwert »Reset by hotline, no reminder question/answer«

Der externe GINA-Benutzer kann sein Kennwort nicht selbstständig zurücksetzen. Er gibt dazu seine Rufnummer an, unter der er für den Support erreichbar ist. Eine Überprüfung durch die Beantwortung einer Sicherheitsfrage ist nicht erforderlich. Beim Erstmaligen Initialisieren des GINA-Benutzerkontos ist es nicht erforderlich, dass der Benutzer eine Sicherheitsfrage angibt. Der Benutzer erhält vom Support-Mitarbeiter ein neues Einmalkennwort zum nächsten Login. Nach dem Login ist es erforderlich, ein neues persönliches Kennwort erfassen. Ein Login mit dem neu gesetzten Kennwort ist nun möglich.

Diese folgenden Möglichkeiten für das Zurücksetzen eines Kennworts können nur im Rahmen der Funktion »Self Service Passwort Management (SSPM)« ausgeführt werden. Siehe GINA Self Service Passwort Management 82

Auswahlwert »Reset by SMS«

Der externe GINA-Benutzer kann ein neues Kennwort via SMS auf sein Mobiltelefon anfordern. Dieses neue Einmalkennwort verwendet der Benutzer für den nächsten Login. Dabei muss er ein neues persönliches Kennwort erfassen. Ein Login mit dem neu gesetzten Kennwort ist nun möglich.

Beim Reset des Kennworts via SMS muss die Mobilfunkrufnummer im Benutzerprofil des Benutzers hinterlegt worden sein.

Beinhaltet ein ausgewähltes Verfahren zur Kennwortrücksetzung die Option SMS, so ist es ebenfalls erforderlich den SMS-Versand im Menü »Mail Processing« einzurichten.

Auswahlwert »Let user choose between hotline and SMS«

Der externen GINA-Benutzer kann zum anfordern eines neuen Kennworts zwischen den beiden Optionen »Hotline« und »SMS« auswählen.

Parameter »Mobile Number«

Beinhaltet die Mobilfunkrufnummer des GINA-Benutzers, falls diese vom Benutzer beim Verwalten seines Benutzerkontos hinterlegt wurde. Für den Support besteht die Möglichkeit dem Benutzer bei Bedarf ein neues One-Time Kennwort (Einmalkennwort) als SMS zu senden. Klicken Sie dazu auf die Schaltfläche »SMS password reset«. Es wird ein neues One-Time Kennwort automatisch durch SEPPmail generiert und via SMS gesendet.

Sektion »User Logs«

In diesem Bereich sehen Sie eine Historie der Benutzerinteraktionen.

* Bei einem Brute-Force Angriff handelt es sich um das Durchprobieren aller möglichen (oder zumindest sehr vieler) Kennwortkombinationen.

6.16 Menüpunkt "PGP public keys"

Wählen Sie den Menüpunkt »PGP public keys«, um die OpenPGP-Benutzerschlüssel der Kommunikationepartner auf der SEPPmail Appliance zu verwalten.

Folgende Vorgänge werden in den kommenden Abschnitten beschrieben:

Übersicht 171
OpenPGP-Schlüssel importieren 171
OpenPGP-Schlüssel herunterladen oder löschen 171

6.16.1 Übersicht Menüpunkt "PGP public keys"

Parameter	Beschreibung
Key ID	Schlüssel-ID des Schlüsselpaars
E-mail addresses	Benutzer-ID des Schlüsselpaars
User Name	Benutzername innerhalb des Schlüsselpaars
Issued on	Ausstellungsdatum des Schlüsselpaars
Expires on	Ablaufdatum des Schlüsselpaars

6.16.2 OpenPGP-Schlüssel importieren

Menü »PGP public keys«

Zum Importieren eines bestehenden OpenPGP-Schlüsselpaar klicken Sie die Schaltfläche »Import PGP key...«. Beim Import eines OpenPGP-Schlüssels können Sie die entsprechende Datei auswählen oder den Schlüssel in Textform einfügen.

6.16.3 OpenPGP-Schlüssel herunterladen oder löschen

Menü »PGP public keys«

Um einen öffentlichen OpenPGP-Schlüssel von der SEPPmail Appliance auf Ihren PC herunterzuladen oder zu löschen, klicken Sie auf die »Key ID« des Schlüssels. Zum Herunterladen des OpenPGP-Keys wählen Sie die Schaltfläche »Download public key«. Möchten Sie hingegen den OpenPGP-Schlüssel löschen, wählen Sie die Schaltfläche »Delete Key«. Zusätzlich können Sie einen Kommentar zu dem PGP public key im Feld Comment erfassen.

6.17 Menüpunkt "X.509 Certificates"

Wählen Sie den Menüpunkt »X.509 Certificates«, um die S/MIME-Benutzerzertifikate der Kommunikationepartner auf der SEPPmail Appliance zu verwalten.

Folgende Vorgänge werden in den kommenden Abschnitten beschrieben:

Übersicht 172
S/MIME-Schlüssel importieren 172
S/MIME-Schlüssel herunterladen oder löschen 173

6.17.1 Übersicht Menüpunkt "X.509 Certificates"

Parameter	Beschreibung
E-mail Address	E-Mail-Adresse innhalb des Zertifikats
Certificate Subject	Identifikation des Zertifikats
Serial Number	Seriennummer des Zertifikats
Issued on	Ausstellungsdatum des Zertifikats
Expires on	Ablaufdatum des Zertifikats

6.17.2 S/MIME-Benutzerzertifikat importieren

Menü »X.509 Certificates«

Manuelles Importieren

Zum Importieren eines bestehenden S/MIME-Benutzerzertifikats klicken Sie die Schaltfläche »Import S/MIME Certificate...«. Wählen Sie zum Import eines S/MIME-Benutzerzertifikats die entsprechende Datei aus. Die zu importieren de Datei darf nicht mit einem Kennwort gesichert sein.

Automatisches Importieren

Neben dem manuellen Importieren von X.509-Benutzerzertifikaten (S/MIME-Signaturen) können diese auch automatisch importiert werden. Dazu werden alle eingehenden S/MIME-signierten E-Mails ausgewertet und gegen die Menge der installierten und als »trusted« klassifizierten Root-CA-Zertifikate geprüft. Wurde eine S/MIME-Signatur von einer vertrauenswürdigen Root-CA ausgestellt, so wird diese Signatur im lokalen Zertifikatsspeicher angelegt. Diese Signatur (public-Key) steht dann global für alle Benutzer zur Verfügung und kann zur Verschlüsselung ausgehender E-Mails verwendet werden.

Das Automatische Importieren von X.509-Benutzerzertifikaten (S/MIME-Signaturen) ist eine Basisfunktion von SEPPmail.

6.17.3 S/MIME-Benutzerzertifikat herunterladen oder löschen

Menü »X.509 Certificates«

Um ein S/MIME-Benutzerzertifikat von der SEPPmail auf Ihren PC herunterzuladen, klicken Sie auf die E-Mail Adresse des Zertifikats. Zum Herunterladen des S/MIME-Benutzerzertifikats wählen Sie die Schaltfläche »Download Certificate. Möchten Sie hingegen das S/MIME-Benutzerzertifikat löschen, wählen Sie die Schaltfläche »Delete Certificate«.

6.18 Menüpunkt "X.509 Root Certificates"

Wählen Sie den Menüpunkt »X.509 Root Certificates«, um die X.509 Root-CA-Zertfikate der vertrauenswürdigen Zertifizierungsstellen auf der SEPPmail Appliance zu verwalten.

Folgende Vorgänge werden in den kommenden Abschnitten beschrieben:

6.18.1 Übersicht Menüpunkt "X.509 Root Certificates"

Die SEPPmail-Appliance beinhaltet bereits im Auslieferungszustand eine umfangreiche Liste mit X.509-Root-Zertifikaten. Diese Liste umfaßt die gängigsten öffentlichen Zertifizierungsstellen. Im produktiven Betrieb kann jedoch es erforderlich sein, diese Liste mit eigenen X.509-Root-Zertifikaten von Kommunikationspartnern zu erweitern oder bereits importierte X.509-Root-Zertifikate zu löschen.

Parameter	Beschreibung
Trust State	aktueller Vertrauenstatus des Zeritikats
Issued to	Ausgestellt für
Issued by	Ausgestellt von
Expires on	Läuft aus am

Parameter »Trust State« - »Vertrauenstatus«

Vertrauensstatus des Zertifikats. Es sind die folgenden Werte möglich:

? (undefined) — Der Vertrauensstatus »?« (undefiniert) wird für alle X.509-Root-Zertifikate vergeben die SEPPmail automatisch von eingehenden S/MIME signierten E-Mails »erntet« und in den Zertifikatsspeicher importiert. Da diese X.509-Root-Zertifikate noch nicht bekannt sind ist es erforderlich, dass die Benutzung durch einen Administrator authorisiert wird.

Hinweis:
Alle neu importierten X.509-Root-Zertifikate die den Status »?« (undefiniert) haben werden im täglichen Status Report aufgeführt der an alle Benutzer der Gruppe »ststisticsadmin« um Mitternach via E-Mail gesendet wird.

trusted — Der Vertrauensstatus »trusted« wird für alle X.509-Root-Zertifikate vergeben die für die produktive Zertifikatsprüfung aller eingehenden signierten E-Mails verwendet werden.

untrusted — Der Vertrauensstatus »untrusted« wird für alle X.509-Root-Zertifikate vergeben die nicht für die produktive Zertifikatsprüfung aller eingehenden signierten E-Mails verwendet werden.

Hinweis:

Die Bezeichner der Spalte »Trust State« sind farblich dargestellt und dienen als Link zur Anzeige von Detailinformationen des jeweiligen Zertifikats. Wenn Sie Detailinformationen zum jeweiligen Zertifikat in diesem Menüpunkt anzeigen wollen, wählen Sie mit dem Mauszeiger den Bezeichner des »Trust State« vom entsprechenden Zertifikat.

Parameter »Issued to« - »Ausgestellt für«

Dieser Wert beschreibt bei X.509-Root-Zertifikaten meist den Betreiber (Firma) der Root-CA bzw. beschreibt die spezifische Verwendung eines Zwischenzertifikats.

Parameter »Issued by« - »Ausgestellt von«

Dieser Wert beschreibt bei X.509-Root-Zertifikaten meist die Firma bzw. den Betreiber der Root-CA der dieses Zertifikat ausgestellt hat.

Parameter »Expires on« - Gültigkeitszeitraum - »Läuft aus am«

Das Ablaufdatum des jeweiligen Zertifikats definiert das Ende der Verwendung des jeweiligen Zertifikats. Nach dem Erreichen bzw. überschreiten des Ablaufdatums wird dieses Zertifikat nicht mehr für die Zertifikatsprüfung und die E-Mail-Signatur verwendet. Importieren Sie ein neues X.509-Root-Zertifikat dieser CA, wenn diese weiterhin verwendet werden soll.

6.18.2 X.509-Root-Zertifikate importieren

Menü »X.509 Root Certificates«

Manuelles Importieren

Zum Importieren eines bestehenden X.509-Root-Zertifikats wählen Sie in der Konfigurationsoberfläche die Schaltfläche »Import S/MIME Root Certificate«. Wählen Sie zum Import eines X.509-Root-Zertifikats die entsprechende Datei aus.

Automatisches Importieren

Neben dem manuellen Importieren von X.509-Root-Zertifikaten können diese auch automatisch importiert werden. Dazu werden alle eingehenden S/MIME-signierten E-Mails ausgewertet. Wurde eine S/MIME-Signatur von einer Root-CA ausgestellt die sich noch nicht im Zertifikatsspeicher von SEPPmail befindet, so wird das bei der S/MIME-Signatur mitgelieferte Root-CA-Zertifikat automatisch importiert. Dieses automatisch importierte Root-CA-Zertifikat wird im Zertifikatsspeicher mit dem Vertrauenstatus »?« (undefined/undefiniert) gekennzeichnet. Alle Root-CA-Zertifikate mit diesem Vertrauenstatus werden nicht für die Überprüfung von S/MIME-Signaturen verwendet.

Zum Aktivieren dieses Zertifikats ist es erforderlich, den Vertrauenstatus auf den Wert »trusted« zu setzen. Über das Vorhandensein eines automatisch importierten Root-CA-Zertifikats mit dem Vertrauenstatus »?« (undefined/undefiniert), wird im täglichen Statusbericht hingewiesen. Dieser wird täglich um 0:00 Uhr an alle Mitglieder der Gruppe »statisticsadmin« via E-Mail gesendet.

6.18.3 X.509-Root-Zertifikate herunterladen oder löschen

Menü »X.509 Root Certificates«

Wählen Sie in der Liste der X.509-Root-Zertifikate (erste Spalte) den Link des Zertifikats aus, welches Sie bearbeiten möchten.

Um ein X.509-Root-Zertifikat von der SEPPmail-Appliance auf Ihren PC herunterzuladen, wählen Sie die Schaltfläche »Download Certificate«. Möchten Sie hingegen ein X.509-Root-Zertifikat löschen, wählen Sie die Schaltfläche »Delete Certificate«.

6.18.4 X.509-Root-Zertifikaten vertrauen

Menü »X.509 Root Certificates«

Um den Vertrauenstatus bestehender X.509-Root-Zertifikate zu verändern, klicken Sie bei einem nicht vertrauten X.509-Root-Zertifikat in der Spalte »Trust State« auf den Link »UNTRUSTED«. Sie können dem X.509-Root-Zertifikat vertrauen, indem Sie auf die Schaltfläche »Trust this certificate« klicken. Nachdem Sie dem X.509-Root-Zertifikat vertraut haben, erhalten Sie die Bestätigungsmeldung »Trust status changed« und das Zertifikat hat neu den Status »trusted«. Zusätzlich können Sie einen Kommentar zu dem »Root CA Zertifikat« im Feld »Comment erfassen«.

Analog dazu wechseln Sie den Vertrauenstatus auf »untrusted«.

6.18.5 X.509-Root-Zertifikate automatisch importieren

Menü »X.509 Root Certificates«

Den manuellen Import von X.509-Root-Zertifikaten ist im Kapitel X.509-Root-Zertifikate importieren 175 beschrieben. SEPPmail bietet zusätzlich die Möglichkeit noch unbekannte X.509-Root-Zertifikate aus eingehenden S/MIME signierten E-Mails automatisch zu importieren. Diese Funktion wird auch als »Certificate harversting«, das Ernten von Zertifikaten, bezeichnet.

Diese automatisch importierten X.509-Root-Zertifikate erhalten immer den Status (Trust State) »undefined«. In der Konfigurationsoberfläche wird dieser Status durch ein »?« Fragezeichen gekennzeichnet. Der Administrator wird über neu importierte X.509-Root-Zertifikate im täglichen System-Report informiert.

Den Vertrauensstatus muss der Administrator manuell in der Konfigurationsoberfläche ändern. Überprüfen Sie bitte vor dem Ändern des Vertrauensstatus das neue X.509-Root-Zertifikat auf Echtheit.

Um einem neuen automatisch importierten X.509-Root-Zertifikat zu vertrauen, wählen Sie in der Konfigurationsoberfläche den Menüpunkt »X.509 Root Certificates«. Anschließend klicken Sie bei einem nicht vertrauten X.509-Root-Zertifikat in der Spalte Trust State auf den Link »?«.

Zum Ändern des Vertrauensstatus verfahren Sie weiter wie im Abschnitt »X.509-Root-Zertifikat vertrauen« 176 beschrieben.

6.19 Menüpunkt "Domain keys"

Wählen Sie den Menüpunkt »Domain keys«, um die OpenPGP-Domainschlüssel und S/MIME-Domainzertifikate der Kommunikationepartner auf der SEPPmail-Appliance zu verwalten.

Folgende Vorgänge werden in den kommenden Abschnitten beschrieben:

6.19.1 Übersicht Menüpunkt "Domain keys"

Die SEPPmail-Appliance bietet die Möglichkeit, automatisch S/MIME-Domainzertifikate anderer SEPPmail Systeme zu importieren. Der Import dieser S/MIME-Public-Domain-keys erfolgt über einen zentralen Update-Dienst der durch die SEPPmail AG bereitgestellt wird.

Beim einrichten einer E-Mail-Domain über die SEPPmail-Konfigurationsoberfläche wird, je nach Einstellung, automatisch ein S/MIME-Domain-Zertifikat erstellt. Der öffentliche Teil dieses Zertifikats (Public key) wird automatisch an einen zentralen Update-Dienst der SEPPmail AG weitergeleitet und nach manueller Prüfung automatisch an alle weltweit installierten SEPPmail-Systeme verteilt.

Sektion »PGP Domain Keys«

Schaltfläche/Parameter	Beschreibung
Import PGP key...	Schaltfläche zum manuellen Importieren bestehender OpenPGP-Domainzertifikate von Kommunikationspartnern
Mail Domain	zum Domain-Public-Key zugeordnete E-Mail-Domain
Key ID	Schlüssel-ID des OpenPGP-Public-key
Issued on	Ausgestellt von
Expires on	Ablaufdatum des Zertifikats

Sektion »SMIME Domain Certificates«

Schaltfläche/Parameter	Beschreibung
Import S/MIME certificate...	Schaltfläche zum manuellen Importieren bestehender S/MIME-Domainzertifikate von Kommunikationspartnern
Mail Domain	zum Domain-Public-Key zugeordnete E-Mail-Domain

Schaltfläche/Parameter	Beschreibung
E-mail Address	E-Mail-Adresse im Domainzertifikat, z.B. domain-confidentiality-authority@customer.com
Serial Number	Seriennummer des Domainzertifikats
Issued on	Ausgestellt von
Expires on	Ablaufdatum des Zertifikats

Sektion »Managed Domain keys«

Schaltfläche/Parameter	Beschreibung
Aktualisierungsstatus	letzter Aktualisierungsversuch der Domainzertifikate vom zentralen Update-Dienst
Update domain certificates...	Schaltfläche, um die Aktualisierung der Domainzertifikate vom zentralen Update-Dienst manuell durchzuführen
Auto-Update SMIME Domain Certificates	Aktiviert/Deaktiviert das automatische Aktualisieren von S/MIME-Domainzertifikaten
Search Domain Certificate...	Suchen nach einem bestehenden S/MIME-Domainzertifikaten im lokalen Domainzertifikatsspeicher für automatisch importierte Managed-Domainzertifikate

Sollten Sie keine automatische Aktualisierung der S/MIME-Domain-keys wünschen, so deaktivieren Sie die Option »Auto-Update SMIME Domain Certificates«.

6.19.2 OpenPGP Domain keys importieren

Menü »Domain keys«

Zum Importieren eines bestehenden OpenPGP-Schlüsselpaars wählen Sie in der Konfigurationsoberfläche die Schaltfläche »Import PGP Key...«. Geben Sie im Feld »Domain name« den zugehörigen E-Mail-Domainnamen an. Sie können dann die entsprechende Datei auswählen oder den Schlüssel in Textform einfügen.

6.19.3 OpenPGP Domain keys herunterladen oder löschen

Menü »Domain keys«

Um einen OpenPGP Domain-key von der SEPPmail Appliance auf Ihren PC herunterzuladen, klicken Sie auf den Namen der angezeigten »E-Mail Domain« des entsprechenden Schlüssels und dann auf die Schaltfläche »Download public key«. Möchten Sie hingegen einen OpenPGP Domain-key löschen, wählen Sie die Schaltfläche »Delete Key«.

6.19.4 S/MIME Domain keys importieren

Menü »Domain keys«

Zum Importieren eines bestehenden S/MIME-Domainzertifikats wählen Sie in der Konfigurationsoberfläche die Schaltfläche »Import S/MIME certificate...«. Geben Sie im Feld »Domain name« den zugehörigen E-Mail-Domainnamen an und wählen Sie zum Import eines S/MIME-Domainzertifikats die entsprechende Datei aus.

6.19.5 S/MIME Domain keys herunterladen oder löschen

Menü »Domain keys«

Um ein vorhandenes S/MIME-Domainzertifikat von der SEPPmail Appliance auf Ihren PC herunterzuladen, klicken Sie auf den Namen der angezeigten »E-Mail-Domain« des entsprechenden Schlüssels und dann auf die Schaltfläche »Download Certificate«. Möchten Sie hingegen ein vorhandenes S/MIME-Domainzertifikat löschen, wählen Sie die Schaltfläche »Delete Certificate«.

6.19.6 Domain keys verwalten

Menü »Domain keys«

Wählen Sie auf die Schaltfläche »Update domain certificates...«, um Domainzertifikate anderer SEPPmail-Appliances mit der eigenen SEPPmail-Appliance abzugleichen. Dieser Abgleich findet automatisch in periodischen Intervallen statt, wenn das Kontrollkästchen »Auto-Update SMIME Domain Certificates« aktiviert ist.

Möchten Sie prüfen, ob ein bestimmtes Domainzertifikat bereits existiert und dessen Details ansehen, geben Sie den entsprechenden E-Mail-Domainnamen im Suchfeld ein und klicken Sie auf die Schaltfläche »Search Domain Certificate...«.

6.20 Menüpunkt "Customers"

Wählen Sie den Menüpunkt »Customers«, das Anlegen einer kundenspezifischen Konfiguration zu ermöglichen. Um diese Funktion zu nutzen ist eine zusätzliche kostenpflichtige Lizenz erforderlich.

Folgende Vorgänge werden in den kommenden Abschnitten beschrieben:

Neuen Kunden erstellen 181
Bestehenden Kunden verwalten 182
Bestehenden Kunden löschen 183

Allgemeiner Informationen

Wenn Sie die Funktion »Multitenancy« aktiviert haben, dann ändert sich der E-Mail-Datenfluss zwischen Absender und Empfänger wie folgt:

- E-Mails werden nur zwischen Absendern und Empfängern übertragen die demselben Kunden zugeordnet sind.
- Wenn ein GINA-Empfänger nicht demselben Kunden zugeordnet ist wie der Absender, dann wird ein neues GINA-Benutzerkonto erstellt unter den Kunden dem auch der Absender zugeordnet ist.
- Im GINA-Portal angemeldete Benutzer können nur an die internen Empfänger Nachrichten versenden die demselben Kunden zugeordnet sind.
- Alle S/MIME-Zertifikate und PGP-Schlüsselpaare für dieselbe E-Mail-Adresse werden mit allen GINA-Benutzerkonten geteilt, die ebenfalls dieselbe E-Mail-Adresse haben.

Jeder Kunde ist einer oder mehreren Managed E-Mail-Domains exklusiv zugewiesen. Eine Managed E-Mail-Domain kann nicht mehreren Kunden zugewiesen werden. Benutzer, die E-Mail-Adressen haben deren Domain einem Kunden zugewiesen wurde, werden automatisch ebenfalls demselben Kunden zugewiesen. Andere Benutzer können einem Kunden manuell zugewiesen werden. GINA-Empfänger müssen einem Kunden immer manuell zugewiesen werden.

GINA-Benutzerkonten und Managed E-Mail-Domains können immer nur einem einzigen Kunden zur gleichen Zeit zugewiesen werden. Keinem Kunden explizit zugewiesene GINA-Benutzerkonten und Managed E-Mail-Domains werden dem »Default Customer« zugewiesen.

Weisen Sie dieselbe GINA-Domain keiner Managed E-Mail-Domains zu, die einem anderen Kunden zugeordnet ist wie die GINA-Domain selbst!

Jedem Kunden können ein oder mehrere Benutzer als spezielle Kunden-Administratoren zugewiesen werden. Diese zugewiesenen Kunden-Aministratoren verwalten die dem Kunden zugewiesenen GINA-Benutzerkonten und die GINA-Domains die den Managed E-Mail-Domains des Kunden zugeordnet sind.

Wenn Sie die Funktion »Multitenancy« das erste Mal aktiviert wird, dann wird auch der Standard-Kunde - »Default Customer« erzeugt. Alle zu diesem Zeitpunkt angelegten Managed E-Mail-Domains, Benutzerkonten und GINA-Benutzerkonten werden dem Standard-Kunden - »Default Customer« zugewiesen. Das System arbeitet weiter wie zuvor.

Nur wenn Kunden angelegt werden und diesen Kunden Managed E-Mail-Domains, Kunden-Administratoren, GINA-Benutzerkonten (optional) und Benutzerkonten zugewiesen werden, verändert sich das Verhalten in der Verarbeitung von E-Mails zuvor beschrieben.

Der spezielle Kunde »No Customer« wird ebenfalls automatisch erzeugt, wenn die Funktion »Multitenancy« das erste Mal aktiviert wird. Diesem Kunden sollen alle GINA-Benutzerkonten zugewiesen werden die sonst keinem Kunden zugewiesen wurden. Diese GINA-Benutzerkonten sollen nicht verwendet werden.

6.20.1 Neuen Kunden erstellen

Menü »Customers«

Zum Erstellen eines neuen Kunden klicken Sie in der Konfigurationsoberfläche die Schaltfläche »Create new customer...«.

Sektion »Customer details«

Parameter	Beschreibung
Customer	Name des Kunden (nicht mehr editierbar)
Customer Name	Bezeichner des Kunden (editierbar)
Customer Admin E-mail	E-Mail-Adressen des Kunden-Administrator (editierbar)
Comment	Kommentar (editierbar)
Creation info	Information zur Erzeugung des Kunden, Benutzer mit Zeitstempel

Sektion »Import backup«

Importieren Sie ein zuvor erzeugtes Kundenbackup. Es wird automatisch ein neuer Kunde angelegt.

6.20.2 Bestehenden Kunden verwalten

Menü »Customers«

Zum Verwalten eines vorhandenen Kunden wählen Sie den Kunden aus und klicken Sie in der Konfigurationsoberfläche die Schaltfläche »Edit...«.

Verwalten eines manuell angelegten Kunden oder des Standard-Kunden »Default Customer«

Sektion »Customer details«

In dieser Sektion können Sie die Detaildaten einsehen und verändern, die Sie beim Anlegen des Kunden erfaßt haben.

Sektion »Customer administrators«

In dieser Sektion können Sie vorhandene Benutzer als Kunden-Administratoren hinzufügen.

Sektion »Assigned managed domains«

In dieser Sektion können Sie vorhandenen Managed E-Mail-Domains diesem Kunden zuordnen.

Sektion »Assigned GINA accounts«

In dieser Sektion können Sie vorhandenen GINA-Benutzerkonten zu diesem Kunden hinzufügen oder entfernen.

Sektion »Backup/Restore«

Schaltfläche »Download«

Manuelles Erzeugen einer Datensicherung zum Speichern auf dem lokalen PC. Die Datensicherung ist mit einem Kennwort geschützt.

Schaltfläche »Change Password«

Ändern des Kennworts für die Datensicherung. Bevor Sie die erste Datensicherung durchführen, setzten Sie das Kennwort zu Schutz der Backupdatei.

Beachten Sie, dass die Backupdatei mit dem Kennwort geschützt ist, welches zum Zeitpunkt der Erstellung des Backups aktuell war.

Schaltfläche »Import Backup File«

Importieren einer zuvor erstellen Datensicherung. Sie benötigen dazu das Kennwort, mit welchem die Backupdatei zum Zeitpunkt der Erstellung gesichert wurde. Ohne das passende Kennwort kann das Backup nicht zurückgesichert werden.

Kundenspezifische Sprachvarianten für das GINA-Subsystem sind nicht Bestandteil der Datensicherung und müssen manuell gesichert und neu installiert werden.

Verwalten des Spezial-Kunden »No Customer«

Beim Kunden »No Customer« handelt es sich um einen speziellen Kunden. Die Verwaltung dieses Kunden erfolgt prinzipiell analog zu manuell angelegten Kunden bzw. dem Kunden »Default Customer« mit den folgenden Ausnahmen:

- Es können keine Managed E-Mail-Domains zugeordnet werden
- Es kann kein Backup erstellt werden

6.20.3 Bestehenden Kunden löschen

Menü »Customers«

Zum Löschen eines vorhandenen Kunden wählen Sie den Kunden aus und klicken Sie in der Konfigurationsoberfläche die Schaltfläche »Delete...«.

Beim Löschen werden alle den Kunden zugewiesenen GINA-Benutzerkonten und Managed E-Mail-Domains dem Standard-Kunden »Default Customer« zugewiesen.

7 Referenz der Regelwerk-Anweisungen

7.1 Kontrollstrukturen - if/else Anweisungen

Die `if/else` Anweisungen sind Kontrollstrukturen und dienen innerhalb des Rulesets der Ablaufsteuerung. Sie sind ein elementarer Bestandteil des Regelwerks. Ist eine Bedingung erfüllt, wird eine Aktionen ausgeführt, sonst wird eine alternative Aktion ausgeführt. Die auszuführende Aktion ist kann immer nur ein Befehl sein. Wenn als Aktion mehrere Befehle ausgeführt werden sollen, so können diese einzelnen Befehle in einem Anweisungsblock zusammengefaßt werden. Ein Anweisungsblock wird innerhalb geschweifter Klammern geschrieben.

Mit `if` wird festgelegt, welche Voraussetzung zur Ausführung einer Aktion erfüllt sein muß. Mit `else` wird eine alternative Aktion eingeleitet, sollte die durch `if` geforderte Bedingung nicht erfüllt sein. Eine `if/else` Anweisung muss nicht durch ein Semikolon abgeschlossen werden. `if/else` Anweisungen können geschachtelt werden.

Aufbau des Befehls

```
if (Bedingung) {
   Anweisungsblock 1;
}
```

oder

```
if (Bedingung) {
   Anweisungsblock 1;
} else {
   Anweisungsblock 2;
}
```

Die `if`-Anweisung bestimmt aufgrund des Rückgabewertes der `Bedingung` den weiteren Verlauf im Programmablauf. Die Bedingung besteht aus einem einzelnen Befehl, die mindestens einen Rückgabewert hat.

`Anweisungsblock 1` wird nur dann ausgeführt, wenn der Rückgabewert positiv ist. Anderenfalls wird, falls vorhanden, ausschließlich `Anweisungsblock 2` ausgeführt.

Beispiel:

```
if (authenticated()) {
} else {
   createaccount('@CREATEGPGKEYS@');
   log(1, 'user account generated');
}
```

Erklärung:

Das Beispiel wertet den Rückgabewert des Befehls `authenticated()` aus. Wenn der interne interne Absender der E-Mail erfolgreich authentifiziert wurde, der Rückgabewert true ist, dann wird ohne weitere Aktion im Programmablauf fortgefahren. Falls die Authentifizierung nicht erfolgreich durchgeführt wurde, wird ein Benutzerkonto für den Absender angelegt.

7.2 Allgemeine Befehle

Parameter die in eckigen Klammern angegeben sind, z.B. [OLDRECIPIENT] sind optional und müssen nicht angegeben werden. Fehlt dieser Parameter wird ein vordefinierter Standardwert bzw. Standardverhalten angewendet.

Innerhalb von Vorlagen stehen die folgenden Variablen zur Verfügung:

Variable	Beschreibung
$header_from	Header-From
$from	From
$header_to	Header-To
$to	To
$header_cc	CC
$mailid	Message ID
$subject	Subject

7.2.1 add_rcpt()

Der Befehl `add_rcpt()` ermöglicht es, eine zusätzliche Empfänger E-Mail-Adresse hinzuzufügen.

Aufbau des Befehls

```
add_rcpt('E-Mail-Adresse');
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Dieser Befehl dient zum Hinzufügen einer zusätzlichen Empfänger E-Mail-Adresse. Die E-Mail-Adresse wird im Envelope hinzugefügt.

Der Rückgabewert ist immer positiv. Dieser Befehl hat 1 Parameter.

Parameter »E-Mail-Adresse«

Dieser Parameter definiert eine E-Mail-Adresse die als zusätzlicher Empfänger im Envelope hinzugefügt

wird..

Beispiel:

```
add_rcpt('recipient@customer.org');
```

Erklärung:

In diesem Beispiel wird ein zusätzlicher Empfänger hinzugefügt. Beim Empfänger erscheint die E-Mail im Posteingang so, als ob diese via BCC gesendet wurde. Der ursprüngliche Empfänger wird nicht verändert.

7.2.2 authenticated()

Der Befehl `authenticated()` überprüft den Identifikationsstatus des Absenders der E-Mail. Der Identifikationsstatus des Absenders beinhaltet die Identität und die Authentifizierung.

Aufbau des Befehls

```
authenticated(['header']);
```

Der Befehl muß mit einem Semikolon abgeschlossen werden. Der Rückgabewert dieses Befehls ist positiv, wenn sich der Absender erfolgreich authentifiziert hat, sonst negativ. Dieser Befehl hat 1 Parameter.

Hinweis:

Authentifiziert bedeutet entweder, dass sich der Benutzer via SMTP authentifiziert hat, oder dass die E-Mail von einem E-Mail-Server kommt, der eine Relay-Berechtigung hat. Die Relay-Berechtigung fügen Sie im Menü »Mail System« -> Sektion »Relaying« hinzu.

Als Benutzer werden die lokalen Named User auf der Appliance bezeichnet.

Parameter »header«

Wenn `header` als Wert angegeben wird, so wird der Benutzer erneut authentifiziert. Dazu wird die E-Mail-Adresse im `FROM`-Feld des Headers benutzt.

Beispiel 1:

```
if (authenticated()) {
} else {
   createaccount('@CREATEGPGKEYS@');
   log(1, 'user account generated');
}
```

Erklärung:

Dieses Beispiel wertet den Rückgabewert des Befehls `authenticated()` aus. Wenn der interne Absender der E-Mail erfolgreich authentifiziert wurde, der Rückgabewert true ist, dann wird ohne weitere Aktion im Programmablauf fortgefahren. Falls die Authentifizierung nicht erfolgreich durchgeführt wurde, wird ein Benutzerkonto für den Absender angelegt.

Beispiel 2:

```
if (authenticated(['header'])) {
} else {
   createaccount('@CREATEGPGKEYS@');
   log(1, 'user account generated');
}
```

Erklärung:

Dieses Beispiel wertet den Rückgabewert des Befehls `authenticated()` aus. Wenn der interne Absender der E-Mail erfolgreich authentifiziert wurde, der Rückgabewert true ist, dann wird ohne weitere Aktion im Programmablauf fortgefahren. Falls die Authentifizierung nicht erfolgreich durchgeführt wurde, wird ein Benutzerkonto für den Absender angelegt.

7.2.3 compare()

Der Befehl `compare()` vergleicht Werte in Headerfeldern.

Aufbau des Befehls

```
compare('Header-Feld', 'Operator', 'Wert');
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Dieser Befehl vergleicht den Inhalt des Parameters `Header-Feld` mit Hilfe des Parameters `Operator` mit dem Parameter `Wert`.

Der Rückgabewert dieses Befehls ist positiv, wenn der Parameter `Wert` mindestens einmal vorkommt, sonst negativ. Dieser Befehl hat 3 Parameter.

Parameter »Header-Feld«

Gibt das `Header-Feld` an, dessen Inhalt gegen den Inhalt des Parameters `Wert` vergleichen werden soll. Als Header-Felder können alle Header in einer E-Mail verwendet werden.

Beispiele für den Parameter »Header-Feld«:

- return-path
- from
- to
- subject
- envelope-to
- etc..

Parameter »Operator«

`equal` : vergleicht auf Gleichheit

`match` : prüft auf das Zutreffen eines regulären Ausdrucks

`substitute` : ist gleich wie `match`, entfernt aber den zutreffenden Teil von `Wert` aus `Header-Feld`

Hinweis:

Codierte Felder werden vor dem Vergleich decodiert. Die Sonderzeichen Tabulator, Wagenrücklauf, Zeilenvorschub und Seitenende werden vor einem Vergleich mit dem Operator `equal` entfernt.

Parameter »Wert«

Gibt den Wert an, gegen den Vergleichen werden soll. Dieser Wert kann auch ein regulärer Ausdruck sein.

Beispiel 1:

```
compare('x-smenc', 'equal', 'yes');
```

Erklärung:

Dieses Beispiel prüft, ob das Header-Feld `x-smenc` exakt den Wert 'yes' beinhaltet. Dies bedeutet nicht, dass der Wert 'yes' lediglich vorhanden ist, sondern, dass der Wert ausschließlich 'yes' beinhaltet.

Beispiel 2:

```
if (compare('to', 'match', '\@cusomer\.com')) {
   tagsubject('[nosign]');
} else {}
```

Erklärung:

Dieses Beispiel prüft bei einer ausgehenden E-Mail im Header-Feld `to` mit dem Operator `match` auf das Vorhandensein der Domain '@customer.com' innerhalb der Empfänger E-Mail-Adresse. Wenn die E-Mail-Adresse des Empfängers die Zeichenkette '@customer.com' enthält, dann ist der Rückgabewert von `compare()` true, im Betreff wird das das Tag '[nosign]' hinzugefügt. Je nach Basiskonfiguration des Ruleset bedeutet dies, dass diese E-Mail nicht signiert wird.

Beispiel 3:

```
compare('subject', 'substitute', '(\s)*\[secure\]');
```

Erklärung:

Dieses Beispiel prüft den Betreff, Header-Feld `subject`, einer E-Mail auf das Vorhandensein des regulären Ausdrucks '(\s)*\[secure\]'. Dieser Ausdruck wird in die Zeichenkette '[secure]' ausgewertet. Wird diese Zeichenkette innerhalb des Betreff gefunden, so wird diese entfernt.

7.2.4 compareattr()

Der Befehl `compareattr()` ermöglicht es, Attribute / Systemvariablen zu prüfen.

Aufbau des Befehls

```
compareattr('Attribut', 'Operator', 'Wert');
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Dieser Befehl vergleicht mit Hilfe des `Operators` den Inhalt des `Header-Feldes` mit dem `Wert`.

Der Rückgabewert ist positiv, sofern mindestens ein Vorkommnis besteht, sonst negativ. Der Befehl hat 3 Paramater.

Parameter »Attribut«

`Attribut` kann die Variable `connect_from` adressieren oder Variablen, die mit `ldap_read()` oder `setuserattr()` geschrieben wurden.

Parameter »Operator«

Für `Operator` stehen zwei verschiedene Operatoren stehen zur Auswahl:

`equal` : vergleicht auf Identität.
`match` : prüft auf das Zutreffen eines regulären Ausdrucks.

Parameter »Wert«

Wert gegen den verglichen werden soll.

Beispiel:

```
if (compareattr('connect_from','equal','172.16.161.1')) {
     log(1,'Message comes from 172.16.161.1'); }
else {
     log(1,'Message does NOT come from 172.16.161.1');
}
```

Erklärung:

In diesem Beispiel wird überprüft, ob die zu verarbeitende E-Mail von einem E-Mail-Server bestimmten Server kommt. Es wird die Systemvariable `connect_from` ausgewertet.

7.2.5 comparebody()

Der Befehl `comparebody()` ermöglicht es, eine E-Mail nach einem angegebenen Wert zu durchsuchen.

Aufbau des Befehls

```
comparebody('Wert');
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Dieser Befehl durchsucht den Nachrichtentext einer E-Mail nach dem angegebenen `Wert`.

Der Rückgabewert dieses Befehls ist positiv, wenn der Parameter `Wert` mindestens einmal vorkommt, sonst negativ. Dieser Befehl hat 1 Parameter.

Parameter »Wert«

Der Parameter `Wert` definiert den Suchbegriff, nach dem innerhalb der E-Mail gesucht wird. `Wert` hat das Format eines regulären Audrucks.

Beispiel:

```
if (comparebody('(\d{1,3}\.){3}\d{1,3}')) {
      log(1, 'Mail contains an IP address');
} else {
      log(1, 'Mail does not contain an IP address');
}
```

Erklärung:

In diesem Beispiel wird innerhalb des Nachrichtentextes einer E-Mail auf das Vorhandensein einer IP-Adresse geprüft. Wird mindestens eine IP-Adresse gefunden, so wird der Log-Eintrag 'Mail contains an IP address' im System-Logger geschrieben. Wird keine IP-Adresse gefunden, so wird der Log-Eintrag 'Mail does not contain an IP address' im System-Logger geschrieben.

7.2.6 disclaimer()

Der Befehl `disclaimer()` fügt einen Textanhang einer bestehenden E-Mail hinzu.

Aufbau des Befehls

```
disclaimer(['Vorlage'], ['Position'], ['force']);
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Dieser Befehl fügt einen Textanhang aus der `Vorlage` einer bestehenden E-Mail hinzu. Wenn eine leere Zeichenfolge als `Vorlage` angegeben ist, wird versucht, anhand der Einstellungen der »Managed Domains« den richtigen Disclaimer zu wählen. Dazu werden die den jeweiligen E-Mail-Domains zugeordneten Disclaimer ausgewertet.

Ist `force` auf `true` gesetzt, so wird jeder ausgehenden E-Mail ein Textanhang hinzugefügt. Dies ist unabhängig davon, ob es sich im eine Antwort-E-Mail handelt oder nicht. Ist `force` nicht angegeben, dann werden die Paramater »Also add disclaimer to replies (in-reply-to header set)« und »Add disclaimer to all outgoing emails« im Menü »Mail Processing« -> Sektion »Ruleset Generator« -> Bereich -> »General Settings« ausgewertet. Statt `true` kann auch `yes` oder `1` verwendet werden.

Der Rückgabewert ist immer positiv. Dieser Befehl hat 3 Parameter.

Parameter »Vorlage«

Definiert den Namen der Vorlage, welche als Textanhang verwendet werden soll. Vorlagen können im Menü »Mail Processing« -> Sektion »Edit Disclaimer« verwaltet werden.

Parameter »Position«

`top` : oberhalb des E-Mail-Body
`bottom` : unterhalb des E-Mail-Body

`Default` : bottom

Parameter »force«

Dieser Paramater erzwingt das hinzufügen eines Textanhangs an eine ausgehende E-Mail.

Option zum Parameter »force«

Mögliche Werte: `true` oder `yes` oder `1`

Beispiel:

```
disclaimer('', 'bottom', 'yes');
```

Erklärung:

In diesem Beispiel wird der Standard Textanhang anhand der Einstellungen innerhalb der »Managed Domains« ausgewählt und am Ende jeder versendeten E-Mail angehängt. Es ist dabei unerheblich, ob es sich um eine Antwort-E-Mail handelt oder nicht.

7.2.7 from_managed_domain()

Der Befehl `from_managed_domain()` ermöglicht es zu prüfen, ob eine E-Mail von einem Absender einer »Managed Domain« gesendet wurde.

Aufbau des Befehls

```
from_managed_domain();
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Der Rückgabewert ist positiv, wenn die E-Mail von einem Absender einer »Managed Domain« versendet wurde, sonst negativ.

Der Befehl hat keinen Parameter.

Beispiel:

```
if (from_managed_domain()) {
     log('1', 'E-Mail is from managed domain');
} else {
     log('1', "E-Mail isn't from managed domain");
}
```

Erklärung:

In diesem Beispiel wird geprüft, ob eine E-Mail von einer unter »Managed Domains« eingetragenen Absender E-Mail-Adresse gesendet wurde.

7.2.8 incoming()

Der Befehl `incoming()` ermöglicht es, das Auslieferungsziel einer E-Mail zu bestimmen.

Aufbau des Befehls

```
incoming();
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Dieser Befehl prüft, ob eine E-Mail lokal ausgeliefert wird. Sind nicht alle Empfänger der E-Mail ausschließlich lokal oder ausschließlich nicht lokal, werden zwei Gruppen gebildet.

Hinweis:

Das Ausliefern einer E-Mail ausschließlich lokal bedeutet, dass diese E-Mail an einen Empfänger weitergeleitet werden kann der unter »Managed Domains« definiert wurde. E-Mails an diese Empfänger werden als ausschließlich lokale Empfänger angesehen und durch den `Anweisungsblock 1` behandelt.

Das Ausliefern einer E-Mail ausschließlich nicht lokal bedeutet, dass die E-Mail an einen externen Empfänger weitergeleitet wird. Diese E-Mail wird wie eine ausgehende E-Mail behandelt und durch den `Anweisungsblock 2` behandelt.

Der Rückgabewert ist für die Gruppe der lokalen Empfänger positiv. Für die Gruppe der nicht lokalen Empfänger ist der Rückgabewert negativ. Dieser Befehl hat keinen Parameter.

Beispiel:

```
if (incoming()) {
     .
     Ruleset-Anweisungen für alle E-Mails die lokal zugestellt werden
können
     .
     Anweisungsblock 1 - Rückgabewert: positiv
     .
} else {
     .
     Ruleset-Anweisungen für alle E-Mails die nicht lokal zugestellt
werden können
     .
     Anweisungsblock 2  - Rückgabewert: negativ
}
```

Erklärung:

In diesem Beispiel wird für eine eingehende E-Mail der `Anweisungsblock 1` ausgeführt. Für eine ausgehende E-Mail wird der `Anweisungsblock 2` ausgeführt.

7.2.9 log()

Der Befehl `log()` ermöglicht es, eine Meldung im Syslog aufzuzeichnen.

Aufbau des Befehls

```
log ('Stufe', 'Eintrag');
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Dieser Befehl sendet den Wert des Parameters `Eintrag` an den System-Logger. Dem Eintrag wird in runden Klammern eine Identifikation (Message-ID) angehängt. Der Wert des Parameters `Stufe` kann einen Wert von 0 bis 7 annehmen und bestimmt die Wichtigkeit des Eintrags.

Die Aufgezeichneten Log-Meldungen können im Menü »Logs« eingesehen werden.

Der Rückgabewert ist immer positiv. Dieser Befehl hat 2 Paramater.

Parameter »Stufe«

n	Bedeutung	n	Bedeutung
0	Debug	4	Error
1	Info	5	Critical
2	Notice	6	Alert
3	Warning	7	Emerg

Parameter »Eintrag«

Geben Sie hier den Text an, der als Log-Eintrag im Syslog aufgezeichnet werden soll.

Beispiel:

```
log ('1', 'Hello World');
```

Header der E-Mail:

```
Date: Fri, 05 Aug 2013 11:40:00 +0200
From: sender@customer.com
To: recipient@customer.de
Subject: Some Topic
Content-Type: text/plain;
Message-Id: <E0D4DE42-DCB5-11D7>
```

Aufzeichnung im Log:

```
Aug 05 11:40:04 test gateway: <E0D4DE42-DCB5-11D7> Hello World
```

Erklärung:

Die Zeichenkette 'Hello World' wird mit der Priorität `info` im Syslog aufgezeichnet.

7.2.10 logheader()

Der Befehl `logheader()` ermöglicht es, den Inhalt einer Headers an den System-Logger zu senden.

Aufbau des Befehls

```
logheader('HEADER');
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Dieser Befehl dient zum Debuggen der Verarbeitung von E-Mails durch die RuleEngine. Es wird der Inhalt des `HEADER` an den System-Logger gesendet.

Der Rückgabewert ist immer positiv. Dieser Befehl hat keine Parameter.

Beispiel:

```
logheader('Message-ID');
```

Erklärung:

In diesem Beispiel wird der Inhalt des Headers 'Message-ID' an den System-Logger gesendet.

7.2.11 normalize_header()

Der Befehl `normalize_header()` ermöglicht es, alle Sonderzeichen in einem Header durch normale ASCII-Zeichen zu ersetzen.

Aufbau des Befehls

```
normalize_header('HEADER');
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Dieser Befehl ersetzt alle Sonderzeichen in `HEADER` durch normale ASCII-Zeichen. Sonderzeichen können z.B. deutsche Umlaute wie ä, ö, ü oder ? sein.

Der Rückgabewert dieses Befehls ist immer positiv. Dieser Befehl hat 1 Parameter.

Parameter »HEADER«

Gibt die Bezeichnung des `HEADER` an.

Beispiele für den Parameter »HEADER«:

- return-path
- from
- to
- subject
- envelope-to
- etc..

Beispiel 1:

```
normalize_header('subject');
```

Erklärung:

In diesem Beispiel wird im Header-Feld `subject` aus der Zeichenkette 'Herr Müller' wird die normalisierte Form 'Herr Mueller'.

Beispiel 2:

```
normalize_header('to');
```

Erklärung:

In diesem Beispiel wird im Header-Feld `to` aus der Zeichenkette '<Bernd Hänsel> bernd.

haensel@customer.com' die normalisierte Form '<Bernd Haensel> bernd.haensel@customer.com'.

7.2.12 notify()

Der Befehl `notify()` ermöglicht es, eine E-Mail-Benachrichtigung bezüglich einer durch SEPPmail verarbeiteten E-Mail zu versenden.

Aufbau des Befehls

```
notify('Empfängeradresse', 'Vorlage', ['From: "System Admin"
<admin@securemail.com>;X-MyHeader: Test']);
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Dieser Befehl erzeugt eine E-Mail-Banachrichtigung und sendet diese an die `Empfängeradresse`.

Die `Empfängeradresse` kann neben einer E-Mail-Adresse auch die Variable `sender` für die Absender-E-Mail-Adresse oder die Variable `admin` für die E-Mail-Adresse des lokalen Administrator sein.

Das Aussehen der E-Mail wird mit der `Vorlage` definiert.

Der dritte Parameter ermöglicht es, zusätzlich eigene Header einzufügen. Mehrere Header können mit einem » ; « getrennt werden.

Der Rückgabewert ist immer positiv. Dieser Befehl hat 3 Parameter.

Parameter »Empfängeradresse«

Dieser Parameter kann die folgenden Werte enthalten:

recipient@customer.com : E-Mail-Adresse, z.B. robert.lander@customer.com

Variablen

`sender` : repräsentiert die E-Mail-Adresse des Absender der verarbeiteten ursprüglichen E-Mail
`admin` : repräsentiert die E-Mail-Adresse des lokalen SEPPmail-Administrators

Hinweis:

Der Platzhalter `admin` bezieht sich auf den lokalen Administrator der Appliance. Dieses definieren Sie im Menü »Mail System« -> Sektion »SMTP settings« -> Parameter »Postmaster address«.

Parameter »Vorlage«

Definiert das Aussehen und den Inhalt der E-Mail-Benachrichtigung. Vorlagen können im Menü »Mail Processing« -> Sektion »Edit Disclaimer« verwaltet werden.

Parameter »Eigene Header«

Dieser Parameter ermöglicht es, zusätzlich eigene Header zu definieren und einzufügen. Mehrere Header können durch ein Semikolon » ; « getrennt werden.

Beispiel für eigene Header:

From : "System Admin" <admin@customer.com>
X-MyHeader : MyOwnHeaderValue

Zusammengefaßte Notation des Parameters mit mehrerem zusätzlichen Headern:

'From: "System Admin" <admin@customer.com>;X-MyHeader: MyOwnHeaderValue'

Der Betreff einer E-Mail, durch den Header `Subject` definiert, kann nicht verändert werden. Dieser Wert ist immer `Notification` und ist fest vorgegeben.

Beispiel 1:

```
notify('sender', 'bounce_noenc', 'From: "System Admin"
<admin@securemail.com>;X-MyHeader: Test');
```

Erklärung:

Bei der Verarbeitung einer E-Mail wird eine zusätzliche E-Mail-Benachrichtigung erzeugt. Diese wird an den Absender der verarbeiteten E-Mail gesendet. Die E-Mail-Adresse des Absenders steht über die Variable `sender` zur Verfügung. Als Nachrichteninhalt wird der Inhalt der Vorlage `bounce_noenc` verwendet. Es werden zusätzlich die Header `From` und `X-MyHeader` mit den jeweiligen Werten eingefügt.

Beispiel 2:

```
notify('revision@customer.com', 'monit_rev', 'From: "System Admin"
<admin@customer.com>;X-MyHeader: Revision');
```

Erklärung:

Bei der Verarbeitung einer E-Mail wird eine zusätzliche E-Mail-Benachrichtigung erzeugt. Diese wird an die E-Mail-Adresse `revision@customer.com` gesendet. Als Nachrichteninhalt wird der Inhalt der Vorlage `monit_rev` verwendet. Es werden zusätzlich die Header `From` und `X-MyHeader` mit den jeweiligen Werten eingefügt.

7.2.13 replace_rcpt()

Der Befehl `replace_rcpt()` ermöglicht es, den/die Empfänger einer E-Mail zu ändern.

Aufbau des Befehls

```
replace_rcpt(['OLDRECIPIENT'], 'NEWRECIPIENT');
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Die Empfänger der verarbeiteten E-Mail können in Abhängigkeit der verwendeten Parameter verändert werden. Jeder Parameter entspricht einem regulären Ausdruck, der als Ergebnis eine E-Mail-Adresse oder einen Teil einer E-Mail-Adresse liefern muss. Wird für den Parameter OLDRECIPIENT der Wert 'admin@customer.com' angenommen, das ist der in der E-Mail enthaltene ursprüngliche Empfänger, und für den Parameter der Wert 'support@customer.com' definiert, so wird die E-Mail an den neuen Empfänger 'support@customer.vom' gesendet.

Ebenfalls können Teile der beiden Parameter als regulärer Ausdruck beschrieben werden. Es kann z.B. nach dem Domainanteil innerhalb der Parameter gesucht werden und dieser durch einen neuen Wert ersetzt werden.

Mehrere Empfänger können mit Strichpunkten » ; « abgetrennt werden.

Der Rückgabewert ist immer positiv. Dieser Befehl hat 2 Parameter.

Parameter »OLDRECIPIENT«

Regulärer Ausdruck der die ursprügliche E-Mail-Adresse oder Teile davon beschreibt.

Parameter »NEWRECIPIENT«

Regulärer Ausdruck der die neue E-Mail-Adresse oder Teile davon beschreibt.

Beispiel:

```
replace_rcpt('\@mydomain\.com', '\@customer\.ch');
```

Erklärung:

In diesem Beispiel wird im Parameter `OLDRECIPIENT` der Domainanteil der ursprünglichen E-Mail-Adresse des/der Empfängers von '@mydomain.com' in den Wert des Paramaters `NEWRECIPIENT`, '@customer.ch', geändert. Der Bestandteil der E-Mail-Adresse vor dem '@' bleibt dabei unverändert. Falls `OLDRECIPIENT` angegeben wird, wird nur dieser Empfänger bzw. der Bestandteil des Empfängers angepaßt.

Falls mehrere E-Mail-Empfängeradressen vorhanden sind, würden alle Empfängeradressen von '@mydomain.com' zu '@mydomain.ch' geändert werden.

7.2.14 replace_sender()

Der Befehl replace_sender() ermöglicht es, den Absender im Envelope einer E-Mail zu verändern.

Aufbau des Befehls

```
replace_sender('neuer sender', ['subst']);
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Dieser Befehl ersetzt den ursprünglichen Absender einer E-Mail im Envelope durch `neuer_senden`. Der Wert für `From` wird dadurch nicht verändert. Der Parameter `subst` entspricht einem regulären Ausdruck. Ist `subst` angegeben, so wird der `subst` entsprechende Teil des ursprünglichen Absenders durch den Wert von `neuer_sender` ersetzt.

Der Rückgabewert ist immer positiv. Dieser Befehl hat 2 Parameter.

Parameter »neuer sender«

Dieser Parameter ist der Wert, durch den die ursprüngliche Absender E-Mail-Adresse im Envelope ersetzt wird. Ist `subst` mit angegeben, so ist `neuer_sender` die Zeichenkette, die für den Teil der E-Mail-Adresse eingesetzt wird auf den `subst` zutrifft.

Parameter »subst«

Regulärer Ausdruck der auf die ursprüngliche Absender E-Mail-Adresse angewendet wird.

Beispiel 1:

```
replace_sender('new_sender@customer.com');
```

Erklärung:

In diesem Beispiel wird die E-Mail-Adresse im Envelope der E-Mail durch 'new_sender@customer.com' ersetzt.

Beispiel 2:

```
replace_sender('@customer.com', '\@customer\.org');
```

Erklärung:

In diesem Beispiel wird der Teil die E-Mail-Adresse im Envelope der E-Mail durch auf den regulären Ausdruck '\@customer\.org' zutrifft durch '@customer.com' ersetzt.

7.2.15 rmatch()

Der Befehl `rmatch()` ermöglicht es zu prüfen, ob ein regulärer Ausdruck auf alle Empfänger zutrifft.

Aufbau des Befehls

```
rmatch('REGEXP');
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Der Rückgabewert dieses Befehls ist positiv, wenn innerhalb der E-Mail erfolgreich auf die `REGEXP`

getestet werden konnte, sonst negativ. Dieser Befehl hat 1 Parameter.

Parameter »REGEXP«

Definiert den regulären Ausdruck auf den getestet werden soll.

Beispiel 1:

```
if (rmatch('\@customer\.org')) {
     notify ('sender', 'info_send_email');
} else {}
```

Erklärung:

In diesem Beispiel wird überprüft, ob die E-Mail-Adresse aller Empfänger einer E-Mail den Domainbestandteil '@customer.org' hat. Ist dies der Fall, dann wird eine E-Mail-Benachrichtigung an den Absender gesendet.

Beispiel 2:

```
if (rmatch('\@customer\.org')) {
     notify ('sender', 'info_send_email', 'From: "System Admin"
<admin@customer.com>');
} else {}
```

Erklärung:

In diesem Beispiel wird überprüft, ob die E-Mail-Adresse aller Empfänger einer E-Mail den Domainbestandteil '@customer.org' hat. Ist dies der Fall, dann wird eine E-Mail-Benachrichtigung an den Absender gesendet. Zusätzlich wird für den Header `From` ein neuer Wert gesetzt.

7.2.16 rmatchsplit()

Der Befehl `rmatchsplit()` ermöglicht es, eine E-Mail durch einen regulären Audruck aufzuteilen.

Aufbau des Befehls

```
rmatchsplit('REGEXP');
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Der reguläre Ausdruck wird auf die gesamte E-Mail angewendet. Das beinhaltet alle Header und den gesamten Body der E-Mail. Eine E-Mail wird in mehrere Gruppen aufgeteilt, wenn auf dem regulären Ausdruck erfolgreich getestet werden konnte. Eine Gruppe, die dem regulären Audruck entspricht und eine weitere Gruppe die dem regulären Ausdruck nicht entspricht. Durch den regulären Ausdruck kann auch eine Vielzahl von Gruppen erzeugt werden. Der Befehl `rmatchsplit()` wird klassisch innerhalb der `if/else` Kontrollstruktur verwendet.

Der Rückgabewert dieses Befehls ist positiv, wenn innerhalb der E-Mail erfolgreich auf die `REGEXP` getestet werden konnte, sonst negativ. Dieser Befehl hat 1 Parameter.

Parameter »REGEXP«

Dieser Parameter definiert den regulären Ausdruck auf dem die E-Mail geprüft wird.

Beispiel:

```
if (rmatchsplit('sales@customer\.com|Invoice')) {
     log(1, 'regex test successful');
} else {
     log(1, 'regex test not successful');
}
```

Erklärung:

In diesem Beispiel wird die E-Mail auf das Vorhandensein der Textbestandteile `sales@customer.com` oder `Invoice` geprüft. Wird einer dieser Textbestandteile innerhalb der gesamten E-Mail gefunden, so wird die Anweisung `log(1, 'regex test successful')` ausgeführt, sonst wird die Anweisung `log(1, 'regex test not successful')` ausgeführt.

7.2.17 rmheader()

Der Befehl `rmheader()` ermöglicht es, eine Header-Zeile innerhalb einer E-Mail zu löschen.

Aufbau des Befehls

```
rmheader('HEADER');
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Hinweis:

Falls mehrere Header mit dem Namen `HEADER` existieren, werden alle Header gelöscht.

Löscht die mit `HEADER` angegebene Header-Zeile innerhalb der E-Mail.

Der Rückgabewert ist immer positiv. Der Befehl hat 1 Parameter.

Parameter »Header«

Gibt das Header-Feld an, welches gelöscht werden soll.

Beispiele für den Parameter »Header-Feld«:

- return-path

- from
- to
- subject
- envelope-to
- etc..

Beispiel:

```
rmheader('X-Greylist');
```

Erklärung:

In diesem Beispiel werden alle `X-Greylist` Header entfernt.

7.2.18 setheader()

Der Befehl `setheader()` ermöglicht es, eine Header-Zeile innerhalb einer E-Mail hinzuzufügen oder zu verändern.

Aufbau des Befehls

```
setheader('HEADER', 'TEXT');
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Dieser Befehl fügt einer E-Mail den `HEADER` mit dem `WERT` hinzu. Falls dieser Header bereits besteht, so wird dieser auf den angegebenen `WERT` geändert.

Hinweis:

Falls mehrere Header mit dem Namen `HEADER` existieren, wird der jeweils erste gefundene Header angepaßt.

Der Rückgabewert ist immer positiv. Dieser Befehl hat 2 Parameter.

Parameter »HEADER«

Gibt das Header-Feld an, welches hinzugefügt oder verändert werden soll.

Beispiele für den Parameter »Header-Feld«:

- return-path
- from
- to
- subject
- envelope-to
- etc..

Beispiel 1:

```
setheader('x-smenc','yes');
```

Erklärung:

In diesem Beispiel wird einer E-Mail der zusätzliche Header `x-smenc` mit dem Wert 'yes' hinzugefügt.

Beispiel 2:

```
setheader('from','info@customer.com');
```

Erklärung:

In diesem Beispiel wird in einer E-Mail das Header-Feld `from` auf dem Wert 'info@customer.com' geändert.

7.2.19 logsubject()

Der Befehl `logsubject()` ermöglicht es, den Inhalt der Betreffzeile einer E-Mail zu protokollieren.

Aufbau des Befehls

```
logsubject();
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Dieser Befehl sendet den Inhalt der Betreffzeile als Log-Info an den System-Logger.

Der Rückgabewert ist immer positiv. Dieser Befehl hat keinen Parameter.

7.2.20 tagsubject()

Der Befehl `tagsubject()` ermöglicht es, dem Betreff einer E-Mail einen Textbestandteil anzuhängen.

Aufbau des Befehls

```
tagsubject('TEXT');
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

In der Betreffzeile einer E-Mail wird den angegebene `TEXT` angehängt.

Der Rückgabewert ist immer positiv. Dieser Befehl hat 1 Parameter.

Parameter »TEXT«

Der Parameter gibt den Text (Zeichenkette) an, der an die Betreffzeile angehängt wird.

Beispiel:

```
tagsubject('[priv]');
```

Erklärung:

In diesem Beispiel wird an den Inhalt der Betreffzeile einer E-Mail die Zeichenkette '[priv]' angehängt.

7.3 Befehle für die Benutzerverwaltung

7.3.1 createaccount()

Der Befehl `createaccount()` ermöglicht es, neue Benutzerkonten zu erstellen.

Aufbau des Befehls

```
createaccount(['KEYS'],['USERID'],['NAME']);
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Als Benutzerkonto wird ein lokales SEPPmail Benutzerkonto bezeichnet. Dieses Benutzerkonto kann im Menü »Users« eingesehen werden. Dieser Befehl wird klassisch innerhalb einer LDAP-Anbindung zum Benutzermanagement eingesetzt.

Der Rückgabewert dieses Befehls ist immer positiv. Dieser Befehl hat 3 Parameter.

Parameter »KEYS«

Dieser Parameter gibt an, welches Schlüsselmaterial beim Erstellen der Benutzerkontos automatisch generiert werden soll. Das Format entspricht einer Bitmaske in Oktalnotation.

Die folgenden Werte stehe zur Verfügung:

Bit 0 : OpenPGP-Schlüsselpaar generieren
Bit 1 : S/MIME-Zertifikat mit der eigenen CA generieren
Bit 2 : S/MIME-Zertifikat via CA-Connector generieren

	Mask	Mask	Mask	Mask	Mask
Bit 0: OpenPGP	x	x	x		
Bit 1: S/MIME mit eigener CA		x			x
Bit 2: S/MIME via CA-Connector			x	x	
Wert für `KEYS`	1	3	5	4	2

Parameter »USERID«

Dieser Parameter gibt die UID des Benutzers an.

Parameter »NAME«

Dieser Parameter gibt des Namen des Benutzers an.

Hinweis:

- Für `USERID` und `NAME` können Variablen benutzt werden, die durch den Befehl `ldap_read()` gesetzt wurden.
- Sonderzeichen in `USERID` und `NAME` werden automatisch ersetzt.

7.3.2 member_of()

Der Befehl `member_of()` ermöglicht es zu prüfen, ob ein Absender einer bestimmten Gruppe zugeordnet ist.

Aufbau des Befehls

```
member_of('group');
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Als Gruppe wird eine lokale SEPPmail Gruppe bezeichnet. Diese Gruppen werden im Menü »Groups« verwaltet.

Der Rückgabewert ist positiv, wenn der Absender der angegebenen Gruppe zugeordnet ist, sonst negativ. Dieser Befehl hat 1 Parameter.

Parameter »group«

Definiert den Namen der Gruppe gegen den die E-Mail-Adresse des Absenders als Mitglied geprüft werden soll.

Beispiel:

```
if (member_of('support')) {
     setheader('x-smenc','yes');
} else {}
```

Erklärung:

In diesem Beispiel wird geprüft, ob der Absender Mitglied der Gruppe 'support' ist. Falls ja, dann wird als Rückgabewert true geliefert, und der Befehl `setheader()` wird ausgeführt. Falls nein wird als Rückgabewert false geliefert.

7.3.3 setuserattr()

Der Befehl `setuserattr()` ermöglicht es, Zusatzinformationen für den aktuellen Benutzer zu speichern.

Aufbau des Befehls

```
setuserattr('ATTR', 'VALUE');
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Es wird eine zusätzliche Variable für den aktuellen Benutzer gesetzt. Der User muß authentifiziert sein.

Der Rückgabewert ist immer positiv. Der Befehl hat 2 Parameter.

Hinweis:

- Für `VALUE` können Variablen benutzt werden, die durch `ldap_read()` gesetzt wurden.
- Es können alle Attribute von InetOrgPerson benutzt werden.
- Die Attribute können im GUI angezeigt werden.

Parameter »ATTR« und »VALUE«

Folgende Systemattribute stehen zur Verfügung:

<table>
<tr><th>ATTR</th><th>VALUE</th></tr>
<tr><td>accountOptions</td><td>Bit 0: User darf nicht verschlüsseln
Bit 2: User darf nicht signieren
<table>
<tr><th></th><th>Mark</th><th>Mask</th><th>Mask</th></tr>
<tr><td>Bit 0: User darf nicht verschlüsseln</td><td>x</td><td></td><td>x</td></tr>
<tr><td>Bit 1: nicht belegt</td><td>-</td><td>-</td><td>-</td></tr>
<tr><td>Bit 2: User darf nicht signieren</td><td></td><td>x</td><td>x</td></tr>
<tr><td>Wert für VALUE</td><td>1</td><td>4</td><td>5</td></tr>
</table>
</td></tr>
<tr><td>Sn</td><td>Name des Benutzers</td></tr>
<tr><td>userPassword</td><td>Kennwort des Benutzers für GUI-Zugriff</td></tr>
<tr><td>Uid</td><td>User ID</td></tr>
</table>

7.4 Befehle für die Zertifikatsverwaltung

7.4.1 attachpgpkey()

Der Befehl `attachpgpkey()` ermöglicht es, den OpenPGP-Public-Key des Absenders an eine E-Mail anzuhängen.

Aufbau des Befehls

```
attachpgpkey();
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Dieser Befehl hängt den OpenPGP-Public-Key des Absenders an eine E-Mail als Dateianhang an.

Der Rückgabewert ist immer positiv. Der Befehl hat keinen Parameter.

7.4.2 has_smime_key()

Der Befehl `has_smime_key()` ermöglicht es zu prüfen, ob der Benutzer einen gültigen privaten S/MIME-Schlüsselbestandteil besitzt.

Aufbau des Befehls

```
has_smime_key();
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Der Rückgabewert ist positiv, wenn der Benutzer einen gültigen privaten S/MIME-Schlüsselbestandteil besitzt, sonst negativ. Der Befehl hat keinen Parameter.

Hinweis:

- Der Rückgabewert ist auch dann negativ, wenn der Benutzer nur abgelaufene S/MIME-Zertifikate besitzt.
- Der Rückgabewert ist auch dann negativ, wenn der Benutzer auf den Status »may not encrypt« gesetzt ist.

7.4.3 smime_create_key()

Der Befehl `smime_create_key()` ermöglicht es, für einen Benutzer ein S/MIME-Zertifikat zu generieren.

Aufbau des Befehls

```
smime_create_key(['SUBJECT']);
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Dieser Befehl generiert ein S/MIME-Zertifikat für einen Benutzer durch die lokale CA. Optional kann das `SUBJECT` für das Zertifikat angegeben werden.

Der Rückgabewert ist immer positiv. Der Befehl hat 1 Parameter.

Parameter »SUBJECT«

Definiert das Subject für das zu erzeugende S/MIME-Zertifikat.

Innerhalb des `SUBJECT` steht die Variable `$sender` zur Verfügung. Über diese Variable steht der Absender der E-Mail zur Verfügung.

Beispiel:

```
smime_create_key('/C=CH/OU=Department/O=Company/emailAddress=$sender');
```

Erklärung:

In diesem Beispiel wird ein S/MIME-Zertifikat über die lokale CA generiert. Das optionale `SUBJECT` wird ebenfalls mitgegeben.

7.4.4 smime_revoke_keys()

Der Befehl `smime_revoke_keys()` ermöglicht es, alle noch nicht abgelaufenen S/MIME-Zertifikate eines Benutzers zu revozieren.

Aufbau des Befehls

```
smime_revoke_keys();
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Der Rückgabewert ist positiv, wenn alle Zertifikate revoziert werden konnten oder abgelaufen sind. Der Rückgabewert ist negativ, wenn mindestens ein Zertifikat nicht revoziert werden konnte, z.B. weil es ein importiertes Zertifikat ist.

Dieser Befehl hat keinen Parameter.

7.4.5 swisssign_create_key()

Der Befehl `swisssign_create_key()` ermöglicht es, es S/MIME-Zertifikat für einen Benutzer von der Zertifizierungsstelle SwissSign zu beschaffen.

Aufbau des Befehls

```
swisssign_create_key();
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Dieser Befehl hat keinen Parameter.

7.5 Befehle für die Handhabung von Nachrichten

7.5.1 archive()

Der Befehl `archive()` ermöglicht es, eine E-Mail erneut zu verarbeiten.

Aufbau des Befehls

```
archive('E-MAIL-ADRESSE');
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Die E-Mail wird innerhalb der Verarbeitung zusätzlich an die `E-MAIL-ADRESSE` gesendet bzw. der E-Mail wird die `E-MAIL-ADRESSE` als weiterer Empfänger hinzugefügt.

Der Rückgabewert ist immer positiv. Der Befehl hat 1 Parameter.

Parameter »E-MAIL-ADRESSE«

E-Mail-Adresse des zusätzlichen Empfängers

Beispiel:

```
archive('recipient@customer.com');
```

Erklärung:

In diesem Beispiel wird die gerade verarbeitete E-Mail zusätzlich an den Empfänger ' recipient@customer.com' gesendet.

7.5.2 bounce()

Der Befehl `bounce()` ermöglicht es, die Verarbeitung einer E-Mail zu veweigern.

Aufbau des Befehls

```
bounce('Vorlage', 'Header als Anlage');
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Dieser Befehl erzeugt eine »Bounce«-E-Mail und löscht die ursprüngliche E-Mail. Das Aussehen der »Bounce«-E-Mail wird durch die `Vorlage` definiert. Der Absender dieser E-Mail ist »admin«. Der E-Mail wird der Header der ursprünglichen E-Mail als Dateianlage angehängt, wenn `Header als Anlage` den booleschen Wert `true` hat. Anstatt `true` kann auch `yes` oder `1` verwendet werden.

Der Befehl hat keinen Rückgabewert. Dieser Befehl hat 2 Parameter.

Hinweis:

- Alle nachfolgenden Befehle werden ignoriert.
- Dieser Befehl kann nicht die Bedingung einer `if/else` Anweisung sein (siehe Abschnitt if/else Anweisungen 184).

Parameter »Vorlage«

Definiert die zu verwendende Vorlage. Vorlagen können im Menü »Mail Processing« -> Sektion »Edit Disclaimer« verwaltet werden.

Parameter »Header als Anlage«

Option zum Parameter »Header als Anlage«

Mögliche Werte: `true`, alternativ `yes` oder `1`

Beispiel:

```
bounce('bounce', 'yes');
```

Erklärung:

Die Auslieferung der E-Mail soll verhindert werden und an den Absender soll eine E-Mail geschickt werden. Der Inhalt der E-Mail ist in der Vorlage bounce definiert. Der E-Mail soll der Header der nicht ausgelieferten E-Mail als Anlage angehängt werden. Die Anweisung sieht wie folgt aus:

7.5.3 deliver()

Der Befehl `deliver()` ermöglicht es, eine E-Mail unmittelbar auszuliefern.

Aufbau des Befehls

```
deliver(['Mailserver[:Port]'|'loop'|'queueless'|'']);
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Dieser Befehl liefert die E-Mail an den angegebenen E-Mail-Server / Port aus. Wird kein Parameter angegeben, so wird die E-Mail dem lokalen Mail-Transport-Agent (MTA) übergeben.

Hinweis:

- Alle nachfolgenden Befehle werden ignoriert.
- Dieser Befehl kann nicht die Bedingung einer `if/else` Anweisung sein (siehe Abschnitt if/else Anweisungen 184).

Der Rückgabewert ist immer positiv. Der Parameter hat 1 Parameter.

Parameter

Optionen zum Parameter

`loop`	:	Das E-Mail wird an den Mailserver zurückgegeben, von welchem es angenommen wurde.
`queueless`	:	Diese Einstellung bewirkt, dass Mails an einzelne Empfänger während der Verarbeitung nicht zwischengelagert werden. Stattdessen wird die eingehende Verbindung erst quittiert, wenn dieabgehende Verbindung quittiert wurde. Wenn beim Versand an mehrere Empfänger die Annahme für einige Empfänger nicht quittiert wird, befinden sich diese Mails kurzzeitig bis zur Quittierung durch die empfangenden Mailserver auf der Appliance.
`keine Option`		Der Befehl wird ohne Parameter aufgerufen.

Beispiel 1:

```
deliver('relay.customer.com:587');
```

Erklärung:

In diese Beispiel wird die E-Mail an den angegebenen E-Mail-Server mit Zielport TCP/587 gesendet.

Beispiel 2:

```
deliver();
```

Erklärung:

In diesem Beispiel wird die E-Mail direkt über den eigenen lokalen E-Mail-Transport-Agent (MTA) ausgeliefert.

7.5.4 drop()

Der Befehl `drop()` ermöglicht es, eine E-Mail zurückzuweisen.

Aufbau des Befehls

```
drop(['CODE'], ['ERROR']);
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Dieser Befehl E-Mail wird nicht mehr verarbeitet die E-Mail und gibt optional einen Errorcode zurück.

Der Befehl hat keinen Rückgabewert. Der Befehl hat 2 Parameter.

Hinweise:

- Weder eine »Bounce«-E-Mail an den Absender noch eine Benachrichtigung an den Empfänger wird erzeugt.
- Alle nachfolgenden Befehle werden ignoriert.
- Dieser Befehl kann nicht die Bedingung einer `if/else` Anweisung sein (siehe Abschnitt if/else Anweisungen 184).

Mit `CODE` und `ERROR` können auch alternative Errorcodes gesetzt werden.

Werden keine Parameter angegeben, so wird der Standard Errorcode mit dem entsprechenden Meldungstext zurückgegeben.

Standard: `CODE` = '555', `ERROR` = 'mail not accepted'

Parameter »CODE«

Gibt den den Errorcode im Form eines numerischen Werts an, z.B. 420.

Parameter »ERROR«

Gibt den Errorcode in Form einer Zeichenkette an, z.B. system temporarily unavailable.

Beispiel:

```
drop('420', 'system temporarily unavailable');
```

Erklärung:

Die E-Mail wird mit dem temporären Fehler »420 system temporarily unavailable« abgewiesen werden.

7.5.5 reprocess()

Der Befehl `reprocess()` ermöglicht es, eine E-Mail erneut zu verarbeiten.

Aufbau des Befehls

```
reprocess();
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Alle an eine E-Mail angehängten E-Mails werden erneut verarbeitet und an den Absender zurückgesendet. Dies kann dann erforderlich sein, wenn sich im Posteingang eines Benutzers noch verschlüsselte E-Mails befinden. Diese können zur erneuten Entschlüsselung an die Appliance gesendet werden und verarbeitet bzw. entschlüsselt werden.

Der Befehl hat keinen Rückgabewert. Dieser Befehl hat keinen Parameter.

Hinweis:

- Die ursprüngliche Message-ID wird aus den neu entschlüsselten E-Mails entfernt.
- Es wird keine »Bounce«-E-Mail an den Absender erzeugt.
- Alle nachfolgenden Befehle werden ignoriert.
- Dieser Befehl kann nicht die Bedingung einer `if/else` Anweisung sein (siehe Abschnitt if/else Anweisungen 184).

Beispiel:

```
if (compare('to', 'match', '(?i)reprocess\@decrypt\.reprocess')) {
     log(1, 'reprocess recipient found - Re-injecting attached
messages');
     reprocess();
     drop('220', 'mesage reprocessed');
} else {}
```

Erklärung:

In diesem Beispiel sendet ein internen Benutzer eine verschlüsselte E-Mail als Anhang in einer nicht verschlüsselten E-Mail an die systemspezifische E-Mail-Adresse `reprocess@decrypt.reprocess`. Die verschlüsselte E-Mail im Anhang wird erneut verarbeitet bzw. es wird versucht diese E-Mail zu entschlüsseln. Es wird ein Log-Eintrag erzeugt. Nach dem Ausführen von `reprocess()` wird die ursprüngliche E-Mail mit `drop()` gelöscht.

7.6 Befehle für die Ver- und Entschlüsselung

7.6.1 decrypt_pgp()

Der Befehl `decrypt_pgp()` ermöglicht es, PGP- verschlüsselte und signierte E-Mails zu entschlüsseln.

Aufbau des Befehls

```
decrypt_pgp();
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Dieser Befehl versucht alle PGP- verschlüsselten und signierten Texte und Anlagen einer E-Mail zu entschlüsseln und deren Signaturen zu prüfen.

Der Rückgabewert ist positiv, wenn mindestens ein Text oder eine Anlage entschlüsselt oder deren Signatur erfolgreich geprüft wurde. Andernfalls ist der Rückgabewert negativ. Dieser Befehl hat keinen Parameter.

7.6.2 decrypt_domain_pgp()

Der Befehl `decrypt_domain_pgp()` ermöglicht es, domainverschlüsselte und signierte PGP-E-Mails zu entschlüsseln.

Aufbau des Befehls

```
decrypt_domain_pgp();
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Dieser Befehl versucht alle PGP- verschlüsselten und signierten Texte und Anlagen einer E-Mail zu entschlüsseln und deren Signaturen zu prüfen die durch den Absender via Domainverschlüsselung verschlüsselt wurden.

Der Rückgabewert ist positiv, wenn mindestens ein Text oder eine Anlage entschlüsselt oder deren Signatur erfolgreich geprüft wurde. Andernfalls ist der Rückgabewert negativ. Dieser Befehl hat keinen Parameter.

7.6.3 domain_pgp_keys_avail()

Der Befehl `domain_pgp_keys_avail()` ermöglicht es, die Verfügbarkeit von PGP-Domian-Public-Keys zu überprüfen.

Aufbau des Befehls

```
domain_pgp_keys_avail('Anwendung');
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Dieser Befehl prüft, ob für alle Empfänger einer E-Mail Domain-PGP-Public-Keys im lokalen Zertifikatsspeicher zur Verfügung stehen.

Der Rückgabewert ist positiv, wenn für alle Empfänger der E-Mail Domain-PGP-Public-Keys vorhanden sind und für den Parameter `Anwendung` der Wert `strict` angegeben wurde, sonst ist der Rückgabewert negativ. Wird für den Parameter `Anwendung` der Wert `auto` angegeben, werden die Empfänger in zwei Gruppen aufgeteilt. Die Gruppe von Empfängern, für die Domain-PGP-Public-Keys vorhanden sind, erhält einen positiven Rückgabewert. Die Gruppe von Empfängern, für die keine Domain-PGP-Public-Keys vorhanden sind, erhält einen negativen Rückgabewert.

Der Befehl hat 1 Parameter.

7.6.4 decrypt_smime()

Der Befehl `decrypt_smime()` ermöglicht es, S/MIME-verschlüsselte E-Mails zu entschlüsseln.

Aufbau des Befehls

```
decrypt_smime();
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Dieser Befehl versucht eine S/MIME-verschlüsselte E-Mail zu entschlüsseln.

Der Rückgabewert ist positiv, wenn die E-Mail entschlüsselt wurde, sonst negativ. Dieser Befehl hat keinen Parameter.

7.6.5 decrypt_domain_smime()

Der Befehl `decrypt_domain_smime()` ermöglicht es, domainverschlüsselte S/MIME-E-Mails zu entschlüsseln.

Aufbau des Befehls

```
decrypt_domain_smime();
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Dieser Befehl versucht eine domainverschlüsselte S/MIME-E-Mail zu entschlüsseln.

Der Rückgabewert ist positiv, wenn die E-Mail entschlüsselt wurde, sonst negativ. Dieser Befehl hat keinen Parameter.

7.6.6 domain_smime_keys_avail()

Der Befehl `domain_smime_keys_avail()` ermöglicht es, die Verfügbarkeit von S/MIME-Domian-Public-Keys zu überprüfen.

Aufbau des Befehls

```
domain_smime_keys_avail('Anwendung');
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Dieser Befehl prüft, ob für alle Empfänger einer E-Mail Domain-S/MIME-Public-Keys im lokalen Zertifikatsspeicher zur Verfügung stehen.

Der Rückgabewert ist positiv, wenn für alle Empfänger der E-Mail Domain-S/MIME-Public-Keys vorhanden sind und für den Parameter `Anwendung` der Wert `strict` angegeben wurde, sonst ist der Rückgabewert negativ. Wird für den Parameter `Anwendung` der Wert `auto` angegeben, werden die Empfänger in zwei Gruppen aufgeteilt. Die Gruppe von Empfängern, für die Domain-S/MIME-Public-Keys vorhanden sind, erhält einen positiven Rückgabewert. Die Gruppe von Empfängern, für die keine Domain-S/MIME-Public-Keys vorhanden sind, erhält einen negativen Rückgabewert.

Der Befehl hat 1 Parameter.

7.6.7 delete_smime_sig()

Der Befehl `delete_smime_sig()` ermöglicht es, die S/MIME-Signatur einer E-Mail zu löschen.

Aufbau des Befehls

```
delete_smime_sig();
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Dieser Befehl löscht eine Signatur aus der signierten E-Mail.

Der Rückgabewert ist positiv, wenn die E-Mail nach dem S/MIME-Verfahren signiert war. Andernfalls ist der Rückgabewert negativ. Dieser Befehl hat keinen Parameter.

Hinweis:

Die Gültigkeit der S/MIME-Signatur wird nicht geprüft.

7.6.8 encrypt_pgp()

Der Befehl `encrypt_pgp()` ermöglicht es, E-Mails via PGP zu verschlüsseln und zu signieren.

Aufbau des Befehls

```
encrypt_pgp('Signatur' [, 'Adresse']);
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Dieser Befehl verschlüsselt alle Texte und Anlagen der E-Mail. Zusätzlich werden sie signiert, wenn die `Signatur` den booleschen Wert `true` hat. Anstatt `true` kann auch `yes` oder `1` verwendet werden. Ist die `Adresse` spezifiziert, wird ausschliesslich der PGP-Public-Key dieses Empfängers zum Verschlüsseln aller E-Mails für alle Empfänger verwendet.

Stehen nicht für alle Empfänger PGP-Public-Keys zur Verfügung, werden zwei Gruppen gebildet.

Der Rückgabewert ist für die Gruppe der Empfänger positiv, für die verschlüsselt werden konnte. Für die Gruppe der Empfänger, für die nicht verschlüsselt werden konnte, ist der Rückgabewert negativ. Dieser Befehl hat 2 Parameter.

Parameter »Signatur«

Option zum Parameter »Signatur«

Mögliche Werte: `true` oder `yes` oder `1`

Parameter »Adresse«

E-Mail-Adresse des Empfängers, dessen PGP-Public-Key zum Verschlüsseln verwendet werden soll.

Beispiel:

```
encrypt_pgp('yes', 'recipient@customer.org');
```

Erklärung:

In diesem Beispiel wird versucht alle Texte und Anlagen einer E-Mail zu verschlüsseln und zu signieren, da `Signatur` den Wert 'yes' hat. Zum Verschlüsseln wird der PGP-Public-Key des mit `Adresse` spezifizierten Empfängers verwendet. In unserem Fall 'recipient@customer.org'.

7.6.9 encrypt_domain_pgp()

Der Befehl `encrypt_domain_pgp()` ermöglicht es, E-Mails via PGP-Domainverschlüsselung zu verschlüsseln.

Aufbau des Befehls

```
encrypt_domain_pgp();
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Dieser Befehl verschlüsselt alle Texte und Anlagen der E-Mail via PGP-Domainverschlüsselung. Stehen nicht für alle Empfänger Domain-PGP-Public-Keys zur Verfügung, werden zwei Gruppen gebildet.

Der Rückgabewert ist für die Gruppe der Empfänger positiv, für die verschlüsselt werden konnte. Für die Gruppe der Empfänger, für die nicht verschlüsselt werden konnte, ist der Rückgabewert negativ. Dieser Befehl hat keinen Parameter.

Beispiel:

```
encrypt_domain_pgp();
```

Erklärung:

In diesem Beispiel wird versucht alle Texte und Anlagen einer E-Mail via PGP-Domainverschlüsselung zu verschlüsseln.

7.6.10 encrypt_smime()

Der Befehl `encrypt_smime()` ermöglicht es, E-Mails via S/MIME zu verschlüsseln.

Aufbau des Befehls

```
encrypt_smime();
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Dieser Befehl verschlüsselt eine E-Mail nach dem S/MIME-Standard. Stehen nicht für alle Empfänger S/MIME-Zertifikate zur Verfügung, werden zwei Gruppen gebildet.

Der Rückgabewert ist für die Gruppe der Empfänger positiv, für die verschlüsselt werden konnte. Für die Gruppe der Empfänger, für die nicht verschlüsselt werden konnte, ist er negativ. Dieser Befehl hat keinen Parameter.

7.6.11 encrypt_domain_smime()

Der Befehl `encrypt_domain_smime()` ermöglicht es, E-Mails via S/MIME-Domainverschlüsselung zu verschlüsseln.

Aufbau des Befehls

```
encrypt_domain_smime();
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Dieser Befehl verschlüsselt alle Texte und Anlagen der E-Mail via S/MIME-Domainverschlüsselung. Stehen nicht für alle Empfänger Domain-S/MIME-Public-Keys zur Verfügung, werden zwei Gruppen gebildet.

Der Rückgabewert ist für die Gruppe der Empfänger positiv, für die verschlüsselt werden konnte. Für die Gruppe der Empfänger, für die nicht verschlüsselt werden konnte, ist der Rückgabewert negativ. Dieser Befehl hat keinen Parameter.

Beispiel:

```
encrypt_domain_smime();
```

Erklärung:

In diesem Beispiel wird versucht alle Texte und Anlagen einer E-Mail via S/MIME-Domainverschlüsselung zu verschlüsseln.

7.6.12 encrypt_webmail()

Der Befehl `encrypt_webmail()` ermöglicht es, eine E-Mail unter Verwendung der GINA-Technologie zu verschlüsseln.

Aufbau des Befehls

```
encrypt_webmail(['TEMPLATE']);
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Dieser Befehl verschlüsselt eine Nachricht via GINA-Technologie für die Empfängeradresse. Die verschlüsselte Nachricht kann anschließend in der RuleEngine weiterverarbeitet werden.

Empfehlung:

Die GINA-Nachricht direkt mit `deliver()` abschicken.

Die Empfängeradresse wird aus der aktuell verarbeiteten Nachricht entnommen.

Falls `TEMPLATE` angegeben ist, wird ein spezielles Template für die GINA-Nachricht verwendet. Falls nicht, wird das Template anhand der Absenderadresse ausgewählt. Als Template wird in diesem Falls das angelegte GINA-Profil bzw. angelegte die GINA-Domain bezeichnet.

Der Rückgabewert ist immer positiv. Der Befehl hat 1 Parameter.

Parameter »TEMPLATE«

Definiert das angelegte GINA-Profil bzw. angelegte die GINA-Domain.

7.6.13 pgp_encrypted()

Der Befehl `pgp_encrypted()` ermöglicht es, eine E-Mail auf PGP-Verschlüsselung zu überprüfen.

Aufbau des Befehls

```
pgp_encrypted();
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Dieser Befehl prüft, ob die vorliegende E-Mail mit dem PGP-Verfahren verschlüsselt ist.

Der Rückgabewert ist positiv, wenn die E-Mail PGP-verschlüsselt ist, sonst negativ. Der Befehl hat keinen Parameter.

7.6.14 pgp_keys_avail()

Der Befehl `pgp_keys_avail()` ermöglicht es, die Verfügbarkeit von PGP-Public-Keys zu überprüfen.

Aufbau des Befehls

```
pgp_keys_avail('Anwendung');
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Dieser Befehl prüft, ob für alle Empfänger einer E-Mail PGP-Public-Keys im lokalen Zertifikatsspeicher zur Verfügung stehen.

Der Rückgabewert ist positiv, wenn für alle Empfänger der E-Mail PGP-Public-Keys vorhanden sind und für den Parameter `Anwendung` der Wert `strict` angegeben wurde, sonst ist der Rückgabewert negativ. Wird für den Parameter `Anwendung` der Wert `auto` angegeben, werden die Empfänger in zwei Gruppen aufgeteilt. Die Gruppe von Empfängern, für die PGP-Public-Keys vorhanden sind, erhält einen positiven Rückgabewert. Die Gruppe von Empfängern, für die keine PGP-Public-Keys vorhanden sind, erhält einen negativen Rückgabewert.

Der Befehl hat 1 Parameter.

7.6.15 pgp_secret_keys_avail()

Der Befehl `pgp_secret_keys_avail()` ermöglicht es, die Verfügbarkeit von PGP-Private-Keys zu überprüfen.

Aufbau des Befehls

```
pgp_secret_keys_avail();
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Dieser Befehl prüft, ob für alle Empfänger einer E-Mail PGP-Private-Keys zur Verfügung stehen.

Der Rückgabewert ist positiv, wenn ein PGP-Private-Keys für den Absender vorhanden ist, sonst negativ.

Dieser Befehl hat keinen Parameter.

7.6.16 smime_keys_avail()

Der Befehl `smime_keys_avail()` ermöglicht es, die Verfügbarkeit von S/MIME-Public-Keys zu überprüfen.

Aufbau des Befehls

```
smime_keys_avail('Anwendung');
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Dieser Befehl prüft, ob für alle Empfänger einer E-Mail S/MIME-Public-Keys im lokalen Zertifikatsspeicher zur Verfügung stehen.

Der Rückgabewert ist positiv, wenn für alle Empfänger der E-Mail S/MIME-Public-Keys vorhanden sind und für den Parameter `Anwendung` der Wert `strict` angegeben wurde, sonst ist der Rückgabewert negativ. Wird für den Parameter `Anwendung` der Wert `auto` angegeben, werden die Empfänger in zwei Gruppen aufgeteilt. Die Gruppe von Empfängern, für die S/MIME-Public-Keys vorhanden sind, erhält einen positiven Rückgabewert. Die Gruppe von Empfängern, für die keine S/MIME-Public-Keys vorhanden sind, erhält einen negativen Rückgabewert.

Der Befehl hat 1 Parameter.

7.6.17 sign_smime()

Der Befehl `sign_smime()` ermöglicht es, eine E-Mail mit der S/MIME-Signatur des Absenders zu versehen.

Aufbau des Befehls

```
sign_smime();
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Der Rückgabewert ist positiv, wenn die Nachricht erfolgreich signiert wurde, sonst negativ. Dieser Befehl hat keinen Parameter.

Beispiel:

```
if (sign_smime()) {
```

```
     log(1, 'sign smime successful');
} else { }
```

Erklärung:

In diesem Beispiel wird eine E-Mail mit der S/MIME-Signatur des Absenders versehen. Es wird weiterhin geprüft, ob dieser Vorgang erfolgreich durchgeführt werden konnte. Falls ja, ist der Rückgabewert `true` und es wird eine Log-Info an den System-Logger gesendet.

7.6.18 smime_signed()

Der Befehl `smime_signed()` ermöglicht es, eine E-Mail auf das Vorhandensein einer S/MIME-Signatur zu überprüfen.

Aufbau des Befehls

```
smime_signed();
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Dieser Befehl prüft, ob die vorliegende E-Mail mit dem S/MIME-Verfahren signiert ist.

Der Rückgabewert ist positiv, wenn die E-Mail S/MIME-signiert ist, sonst negativ. Dieser Befehl hat keinen Parameter.

7.6.19 smime_encrypted()

Der Befehl `smime_encrypted()` ermöglicht es, eine E-Mail auf S/MIME-Verschlüsselung zu überprüfen.

Aufbau des Befehls

```
smime_encrypted();
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Dieser Befehl prüft, ob die vorliegende E-Mail mit dem S/MIME-Verfahren verschlüsselt ist.

Der Rückgabewert ist positiv, wenn die E-Mail S/MIME-verschlüsselt ist, sonst negativ. Dieser Befehl hat keinen Parameter.

7.6.20 validate_smime_sig()

Der Befehl `validate_smime_sig()` ermöglicht es, die S/MIME-Signatur einer E-Mail auf Gültigkeit zu prüfen.

Aufbau des Befehls

```
validate_smime_sig('Zertifikat speichern');
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Dieser Befehl prüft die S/MIME-Signatur einer E-Mail auf Gültigkeit. Zusätzlich zur Signaturprüfung kann das Zertifikat in den Zertifikatsspeicher der Appliance importiert werden, wenn für den Parameter `Zertifikat speichern` der Wert `true` gesetzt wurde. Statt `true` kann auch `yes` oder `1` verwendet werden.

Der Rückgabewert ist positiv, wenn alle der folgenden Punkte zutreffen:

- Die E-Mail wurde mit dem S/MIME-Verfahren signiert.
- Die E-Mail ist vollständig und unverändert.
- Die E-Mail wurde mit einem S/MIME-Zertifikat signiert, das von einer als vertrauenswürdig eingestuften Certificate Authority (CA) ausgestellt wurde.
- Das zur Anbringung der Signatur verwendete S/MIME-Zertifikat ist weder auf einer der Appliance bekannten »Revocation list« (CRL) aufgeführt, noch ist dessen Ablaufdatum überschritten.

Falls einer der obigen Punkte nicht zutrifft, ist der Rückgabewert negativ. Dieser Befehl hat 1 Parameter.

Parameter »Zertifikat speichern«

Option zum Parameter »Zertifikat speichern«

Mögliche Werte: `true` oder `yes` oder `1`

Beispiel:

```
if (validate_smime_sig('true')) {
     log(1, 'smime signed valid');
} else {
     log(1, 'smime signed, but signature invalid');
}
```

Erklärung:

In diesem Beispiel wird die S/MIME-Signatur einer E-Mail auf Gültigkeit überprüft. Ist der Rückgabewert von `validate_smime_sig()` positiv, dann wird der Log-Eintrag 'smime signed valid' geschrieben. Sonst wird der Log-Eintrag 'smime signed, but signature invalid' geschrieben.

7.6.21 webmail_keys_avail()

Der Befehl `webmail_keys_avail()` ermöflicht es zu prüfen, on ein GINA-Benutzerkonto zur vorhanden ist.

Aufbau des Befehls

```
webmail_keys_avail('Anwendung');
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Dieser Befehl prüft, ob für alle Empfänger einer E-Mail ein GINA-Benutzerkonto zur Verfügung steht. Ist die `Anwendung` des Befehls `strict`, so ist der Rückgabewert nur dann positiv, wenn für alle Empfänger GINA-Benutzerkonten vorhanden sind. Ist die Anwendung `auto`, teilt der Befehl die Empfänger in zwei Gruppen auf und gibt jeder Gruppe den entsprechenden Rückgabewert mit.

Dieser Befehl hat 1 Parameter.

7.6.22 webmail_keys_gen()

Der Befehl `webmail_keys_gen()` ermöglicht es, GINA-Benutzerkonten zu erzeugen.

Aufbau des Befehls

```
webmail_keys_gen(['Empfängeradresse'], ['Länge des Kennworts'],
['NoPwEmailIsSmsSend']);
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Dieser Befehl generiert ein GINA-Benutzerkonto und schickt das Initialisierungskennwort an den Absender der ursprünglichen E-Mail oder an `Empfängeradresse`, falls diese angegeben ist.

Der Rückgabenwert ist immer positiv. Der Befehl hat 3 Parameter.

Parameter »Empfängeradresse«

Definiert die E-Mail-Adresse, an die die E-Mail mit dem Initialisierungskennwort gesendet werden soll.

Parameter »Lange des Kennworts«

Definiert die Länge des Kennworts: 0 für leeres Kennwort. Wird der Parameter nicht angegeben, wird der Standardwert verwendet. Dieser kann über die Konfigurationsoberfläche eingesehen und verändert werden.

Parameter »NoPwEmailIsSmsSend«

Option zum Parameter »NoPwEmailIsSmsSend«

Mögliche Werte: `true` oder `yes` oder `1`

Beispiel:

```
webmail_keys_gen('', '8');
```

Erklärung:

In diesem Beispiel wird ein GINA-Benutzerkonto erzeugt. Der Absender der ursprünglichen E-Mail

erhält eine E-Mail-Benachrichtigung mit dem Initialisierungskennwort. Das Kennwort für dieses GINA-Benutzerkonto muss mindestens 8 Stellen haben.

7.6.23 pack_mail()

Der Befehl `pack_mail()` ermöglicht es, eine ausgehende E-Mail für die Weiterleitung an ein GINA-Relay-System zu packen.

Aufbau des Befehls

```
pack_mail('E-Mail-Addr', ['Domainsignatur']);
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Dieser Befehl packt eine E-Mail für die Weiterleitung an ein GINA-Relay-System. E-Mail-Addr definiert die E-Mail-Adresse des GINA-Relay-Systems. Ist der optionale Parameter Domainsignatur true, so wird die gepackte E-Mail zusätzlich signiert. Statt `true` kann auch `yes` oder `1` verwendet werden.

Der Rückgabewert ist positiv, wenn das Packen der E-Mail erfolgreich war, sonst negativ. Der Befehl hat 2 Parameter.

Parameter »E-Mail-Addr«

Definiert die E-Mail-Adresse des GINA-Relay-Systems

Paramater »Domainsignatur«

Option zum Parameter »Domainsignatur«

Mögliche Werte: `true` oder `yes` oder `1`

Beispiel:

```
pack_mail('gina-relay@customer.org', 'yes');
```

Erklärung:

In diesem Beispiel wird die ausgehende E-Mail zur Weiterleitung an ein GINA-Relay-System gepackt. Daraus wird eine neue E-Mail-Nachricht erzeugt und an die Ziel-E-Mail-Adresse des GINA-Relay-Systems gesendet. Zusätzlich wird diese E-Mail-Nachricht mit dem Domainzertifikat signiert.

7.6.24 unpack_mail()

Der Befehl `unpack_mail()` ermöglicht es, eine gepackte E-Mail auf einem GINA-Relay-System zu entpacken.

Aufbau des Befehls

```
unpack_mail();
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Der Rückgabewert ist immer positiv. Dieser Befehl hat keine Parameter.

7.7 Befehle für LDAP (Zugriff auf externe Quellen)

7.7.1 ldap_compare()

Der Befehl `ldap_compare()` ermöglicht es, einen in einem LDAP-Verzeichnis abgelegten Wert mit einem angegebenen Attribut zu vergleichen.

Aufbau des Befehls

```
ldap_compare('URI;USER;PASSWORD;BASEDN;FILTER', 'ATTR', 'VALUE');
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Dieser Befehl baut eine Verbindung zu einem LDAP-Server auf und prüft den Wert eines Attributs.

Der Rückgabewert ist positiv, wenn `VALUE` im Attribut vorhanden ist, sonst negativ. Dieser Befehl hat 3 Parameter.

Parameter

Parameter	Beschreibung
URI	Die IP-Adresse oder der Name des LDAP-Servers. Es können auch zwei mit Komma getrennte Werte angegeben werden: In diesem Fall wird automatisch auf den zweiten Server zugegriffen, wenn der erste nicht erreicht werden kann.
USER	Der User, welcher für den Zugriff verwendet werden soll
PASSWORD	Das Passwort des Users
BASEDN	Die Base DN (Distinguished Name) für die Abfrage
FILTER	Der Filter für die Abfrage
ATTR	Das Attribut, welches abgefragt werden soll
VALUE	Der Wert, welcher im Attribut vorkommen soll

Beispiel:

Es soll geprüft werden, ob der aktuelle Benutzer der Gruppe »Meinegruppe« angehört.

Die Anweisung sieht wie folgt aus:

```
ldap_compare('192.168.10.10;CN=Peter Mueller,OU=SBSUsers,OU=Users,
OU=MyBusiness,DC=Firma,DC=local;mypassword;OU=SBSUsers,OU=Users,
OU=MyBusiness,DC=Firma,DC=local;(mail=$sender)','memberOF',
Meinegruppe');
```

Erklärung:

- Sollte das angegebene Attribut oder der gesuchte Eintrag nicht existieren, so ist der Rückgabewert negativ.
- Sollten mehrere Einträge gefunden werden, so wird nur der erste ausgewertet.
- Sollten mehrere Attribute vorhanden sein, so werden alle Attribute ausgewertet (Multi value).
- Falls keiner der angegebenen LDAP-Server erreichbar ist, so wird die Mail mit einem temporären Fehler abgewiesen.

7.7.2 ldap_read

Der Befehl ldap_read() ermöglicht es, einen in einem LDAP-Verzeichnis abgelegten Wert auszulesen.

Aufbau des Befehls

```
ldap_read('URI;USER;PASSWORD;BASEDN;FILTER' ,'ATTR', 'VAR');
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Dieser Befehl baut eine Verbindung zu einem LDAP-Server auf und speichert den Wert des abgefragten Attributs in der Variable `VAR`. Der Rückgabewert ist positiv, wenn der Variablen `VAR` ein Wert zugewiesen werden kann, sonst negativ. Dieser Befehl hat 3 Parameter.

Parameter

Parameter	Beschreibung
URI	Die IP-Adresse oder der Name des LDAP-Servers. Es können auch zwei mit Komma getrennte Werte angegeben werden: In diesem Fall wird automatisch auf den zweiten Server zugegriffen wenn, der erste nicht erreicht werden kann.
USER	Der User, welcher für den Zugriff verwendet werden soll
PASSWORD	Das Passwort des Users
BASEDN	Die Base DN (Distinguished Name) für die Abfrage
FILTER	Der Filter für die Abfrage
ATTR	Das Attribut, welches abgefragt werden soll
VAR	Variable, in welcher das Attribut gespeichert werden soll

Beispiel:

Es soll der Wert des Attributs »name« aus einem LDAP-Verzeichnis ausgelesen werden. Dieser soll in der Variable »name« abgespeichert werden.

```
ldap_read('192.168.10.10;CN=Peter Mueller,OU=SBSUsers,OU=Users,
```

```
OU=MyBusiness,DC=Firma,DC=local;mypassword;OU=SBSUsers,OU=Users,
OU=MyBusiness,DC=Firma,DC=local; (mail=$sender)','name','name'););
```

Erklärung:

- Sollte das angegebene Attribut oder der gesuchte Eintrag nicht existieren, so wird der Variable ein leerer Wert zugewiesen.
- Sollten mehrere Einträge (Objekte) gefunden werden, so wird nur der erste ausgewertet.
- Sollten mehrere Attribute vorhanden sein, so werden alle Attribute ausgelesen und mit Strichpunkten ";" abgetrennt der Variablen zugewiesen (Multi value Attribut).
- Falls keiner der angegebenen LDAP-Server erreichbar ist, so wird die Mail mit einem temporären Fehler abgewiesen.

7.7.3 ldap_getcerts()

Der Befehl `ldap_getcerts()` ermöglicht es, S/MIME-Public-Keys bei einem LDAP-Verzeichnisdienst abzurufen.

Aufbau des Befehls

```
ldap_getcerts('URI;USER;PASSWORD;BASEDN');
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Dieser Befehl ermöglicht es, S/MIME-Public-Key für jeden Empfänger einer E-Mail bei einem LDAP-Verzeichnisdienst anzurufen.

Der Rückgabewert ist immer positiv. Dieser Befehl hat 1 Parameter.

Paramater

Beispiel:

`URI` : ldap-directory.domain.tld
`USER` : Benutzername zur Anmeldung am LDAP-Verzeichnis
`PASSWORD` : Kennwort zur Anmeldung am LDAP-Verzeichnis
`BASEDN` : ou=pki-participant,dc=pki,dc=domain,dc=tld

Parameter	Beschreibung
URI	Die IP-Adresse oder der Name des LDAP-Servers. Es können auch zwei mit Komma getrennte Werte angegeben werden: In diesem Fall wird automatisch auf den zweiten Server zugegriffen wenn, der erste nicht erreicht werden kann.
USER	Der User, welcher für den Zugriff verwendet werden soll
PASSWORD	Das Passwort des Users
BASEDN	Die Base DN (Distinguished Name) für die Abfrage

Beispiel:

```
ldap_getcerts('ldap-directory.domain.tld;;;ou=pki-participant,dc=pki,
dc=domain,dc=tld');
```

Erklärung:

In diesem Beispiel wird für den Empfänger einer E-Mail der S/MIME-Public-Key bei einem LDAP-Verzeichnisdienst abgefragt. Der Zugang zu diesem LDAP-Verzeichnisdienst ist öffentlich, deshalb sind keine Anmeldeinformationen erforderlich.

7.7.4 ldap_getpgpkeys()

Der Befehl `ldap_getpgpkeys()` ermöglicht es, PGP-Public-Keys bei einem LDAP-Verzeichnisdienst abzurufen.

Aufbau des Befehls

```
ldap_getpgpkeys('URI;USER;PASSWORD;BASEDN');
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Dieser Befehl ermöglicht es, PGP-Public-Key für jeden Empfänger einer E-Mail bei einem LDAP-Verzeichnisdienst anzurufen.

Der Rückgabewert ist immer positiv. Dieser Befehl hat 1 Parameter.

Paramater

Beispiel:

`URI` : ldap-directory.domain.tld
`USER` : Benutzername zur Anmeldung am LDAP-Verzeichnis
`PASSWORD` : Kennwort zur Anmeldung am LDAP-Verzeichnis
`BASEDN` : ou=pki-participant,dc=pki,dc=domain,dc=tld

Parameter	Beschreibung
URI	Die IP-Adresse oder der Name des LDAP-Servers. Es können auch zwei mit Komma getrennte Werte angegeben werden: In diesem Fall wird automatisch auf den zweiten Server zugegriffen wenn, der erste nicht erreicht werden kann.
USER	Der User, welcher für den Zugriff verwendet werden soll
PASSWORD	Das Passwort des Users
BASEDN	Die Base DN (Distinguished Name) für die Abfrage

Beispiel:

```
ldap_getpgpkeys('ldap-directory.domain.tld;;;ou=pki-participant,dc=pki,
dc=domain,dc=tld');
```

Erklärung:

In diesem Beispiel wird für den Empfänger einer E-Mail der PGP-Public-Key bei einem LDAP-Verzeichnisdienst abgefragt. Der Zugang zu diesem LDAP-Verzeichnisdienst ist öffentlich, deshalb sind keine Anmeldeinformationen erforderlich.

7.8 Befehle für Content Management

7.8.1 iscalendar()

Der Befehl `iscalendar()` ermöglicht es, eine E-Mail auf das Vorhandensein des Mime-Type »text/calendar« zu prüfen.

Aufbau des Befehls

```
iscalendar();
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Der Befehl prüft, ob die E-Mail den Mime-Type »text/calendar« beinhaltet. Falls ja, ist der Rückgabewert positiv, sonst negativ. Dieser Befehl kann benutzt werden, um zu verhindern, dass E-Mails mit Kalendereintrgungen z.B. Einladungen, Termine, Besprechungsanfragen signiert werden. Microsoft Outlook kann z.B. nicht mit signierten Kalendereinträgen umgehen.

Dieser Befehl hat keine Parameter.

7.8.2 isspam()

Der Befehl `isspam()` ermöglicht es, eine E-Mail auf SPAM zu überprüfen.

Aufbau des Befehls

```
isspam('MARKLEVEL', 'TAG', 'REJECTLEVEL');
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Der Rückgabewert dieses Befehls ist immer positiv. Dieser Befehl hat 3 Parameter.

Parameter »MARKLEVEL«

Dieser Parameter definiert den Punktwert, ab dem eine E-Mail als SPAM-E-Mail markiert wird. Zum Markieren wird das angegebene `TAG` verwendet.

Wertebereich : 0.5 - 9.5
Schrittweite : 0.5

Parameter »TAG«

Dieser Parameter definiert einen Wortbestandteil (`TAG`) der zur Markierung einer E-Mail als SPAM an den Betreff angehängt wird.

Beispiel für diesen Parameter: [SPAM]

Parameter »REJECTLEVEL«

Dieser Parameter definiert den Punktwert, ab dem eine E-Mail als SPAM abgewiesen wird.

Wertebereich : 0.5 - 9.5
Schrittweite : 0.5

Beispiel:

```
isspam('2.5', '[SPAM]', '4.5');
```

Erklärung:

In diesem Beispiel wird eine E-Mail auf SPAM überprüft. Der Parameter für `MARKLEVEL` hat den Wert '2.5'. Wird bei der SPAM-Prüfung dieser Schwellwert erreicht bzw. überschritten, dann wird die E-Mail mit dem `TAG` '[SPAM]' markiert. Das `TAG` wird an den Betreff angehängt. Wird der Schwellwert von '4.5' für `REJECTLEVEL` erreicht oder überschritten, dann wird die E-Mil abgewiesen und nicht empfangen.

7.8.3 partoftype()

Der Befehl `partoftype()` ermöglicht es, den Dateityp von E-Mail-Dateianlagen zu bestimmen.

Aufbau des Befehls

```
partoftype('Typ', 'Handlung', 'Archivinhalte prüfen');
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Dieser Befehl prüft, ob die Dateianlagen einer E-Mail einem bestimmten `Typ` entsprechen. Die `Handlung` definiert, was mit den Datenanlagen passiert, wenn die Prüfung auf den `Typ` positiv ist. Die Inhalte von Archivdateien werden durchsucht, wenn `Archivinhalte prüfen` den booleschen Wert `true` hat. Statt `true` kann auch `yes` oder `1` verwendet werden.

Der Rückgabewert ist immer dann `positiv`, wenn das Ergebnis mindestens einer Prüfung der Dateianlagen einer E-Mail positiv ist, sonst ist er `negativ`. Der Befehl hat 3 Parameter.

Parameter »Typ«

Weitere Informationen zum Parameter `Typ` sind im Abschnitt Liste der Dateitypen 237 zu finden.

Parameter »Handlung«

Für den Parameter `Handlung` stehen folgenden Optionen zur Verfügung:

`info` : stellt das Resultat für die folgenden Befehle zu Verfügung
`delete` : entfernt zusätzlich die entsprechende Dateianlage aus der E-Mail

Parameter »Archivinhalte prüfen«

Option zum Parameter »Archivinhalte prüfen«

Mögliche Werte: `true`, alternativ `yes` oder `1`

Beispiel:

```
partoftype('EXE', 'delete', 'true');
```

Erklärung:

In diesem Beispiel wird eine E-Mail auf das Vorhandensein von Dateianhängen des `Typ` 'EXE' überprüft. Wird ein Dateianhang gefunden, so wird dieser aus der E-Mail entfernt. Enthält die E-Mail als Dateianhang eine Archivdatei, so wird diese ebenfalls durchsucht. Wird innerhalb der Archivdatei eine Datei vom `Typ` 'EXE' gefunden, so wird die Datei aus dem Archiv entfernt.

7.8.4 vscan()

Der Befehl vscan() ermöglicht es, alle Datenanlagen einer E-Mail auf Viren zu prüfen.

Aufbau des Befehls

```
vscan('E-Mail-Addr-für-Benachrichtigung');
```

Der Befehl muß mit einem Semikolon abgeschlossen werden.

Dieser Befehl prüft alle Dateianlagen einer E-Mail auf bekannte Viren. Wird ein Virus gefunden, dann wird eine E-Mail-Benachrichtigung an `E-Mail-Addr-für-Benachrichtigung` gesendet. Ein nachfolgender Ruleset-Befehl muss diese E-Mail weiter behandeln.

Der Rückgabewert ist immer dann positiv, wenn das Ergebnis mindestens einer Prüfung der Dateianlagen einer E-Mail positiv ist, sonst ist er negativ. Der Befehl hat 1 Parameter.

Parameter »E-Mail-Addr-für-Benachrichtigung«

Definiert die E-Mail-Adresse an die eine Benachrichtigung bei Virenfund gesendet wird.

Beispiel:

```
vscan('antivirus-admin@customer.com');
```

Erklärung:

In diesem Beispiel wird eine E-Mail-Benachrichtigung an 'antivirus-admin@customer.com' gesendet, wenn ein Virus gefunden wurde.

7.9 Dateitypen

7.9.1 Liste der Dateitypen

Folgende Dateitypen werden unterschieden:

ID	Beschreibung
BMP	PC Bitmap
BZIP	BZIP Compressed
CAB	Microsoft CAB file
COM	MSDOS Computable
EMF	Enhanced Windows Metafile
EXE	MSDOS Executable
FAX	G3 Fax
GIF	GIF Image
GZIP	GZIP Compressed
ICO	Windows Icon
ISO9660	ISO 9660 CD-ROM
JPEG	JPEG Image
JPG2000	JPEG 2000 Image
LHA	LHa 2.x? Archive
LHARC	LHarc 1.x Archive
LWF	LuraWave Image
MPEG.L3	MPEG Layer 3
MPEG.SYS	MPEG System Stream
MPEG.VID	MPEG Video
MS.ASF	Microsoft ASF
MS.OFF	MS Office document
MS.XLS	MS Excel 5.0 Worksheet
NIFF	NIFF Image
PBMPLUS	PBMPLUS Bitmap
PCX	Z-Soft Image
PDF	PDF Document
PNG	PNG Image
RAR	RAR Archive
RIFF.ANI	MS RIFF Animated Cursor
RIFF.AVI	MS RIFF Audio Video Interleave
RIFF.DIB	MS RIFF DIB Bitmap
RIFF.MID	MS RIFF MIDI File
RIFF.MMF	MS RIFF Multimedia Movie
RIFF.WAV	MS RIFF Wave Audio
RTF	Rich Text Format
TAR	TAR Archive

ID	Beschreibung
TARGA	TARGA Bitmap
TIFF	TIFF Image
ZIP	PKZIP Archive
ZOO	Zoo Archive

Liste der Dateitypen

7.9.2 Gruppen von Dateitypen

Folgende Gruppen von Dateitypen werden unterschieden:

ID	Beschreibung	Beinhaltete Dateitypen
ARCHIVES	Archivdateien	ZIP ZIP.SFX RAR LHARC LHA SQUISH UC2 ZOO TAR CAB BZIP GZIP
EXE	Ausführbare Dateien	EXE.PE EXE COM
FS	Dateisysteme	ISO9660 HISIERRA
IMAGES	Bilder	JPEG BMP TIFF PNG GIF TARGA PBMPLUS NIFF FAX PCX LWF ICO JPG2000 EMF
MEDIA	Multimedia	RIFF.WAV RIFF.AVI RIFF.ANI RIFF.MID RIFF.MMF RIFF.DIB RIFF RIFX MPEG.VID MPEG.SYS MPEG.L3 MS.ASF
OFFICE	Office-Dokumente	RTF PDF MS.OFF MS.XLS

Gruppen von Dateitypen